Sun Java Enterprise System Glossary

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–3875–14
March 2007

070328@17039

Preface

This glossary identifies terms and definitions for Java Enterprise System.

Additionally, this glossary identifies the following:

- Acronyms
- Parts of speech where a term is used, for example, as both a noun and a verb. Abbreviations include the following:
  - adj. – Adjective
  - n. – Noun
  - v. – Verb
- Numbered usages in different products or technologies
- Cross-references
- Synonyms
- Contrasting terms
- Pronunciation key, if appropriate

Typographic Conventions

The following table describes the typographic changes that are used in this book.

TABLE 1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

TABLE 1 Typographic Conventions *(Continued)*

Typeface	Meaning	Example
AaBbCc123	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
AaBbCc123	A placeholder to be replaced with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized (note that some emphasized items appear bold online)	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file.

Shell Prompts in Command Examples

The following table shows default system prompts and superuser prompts.

TABLE 2 Shell Prompts

Shell	Prompt
C shell on UNIX and Linux systems	`machine_name%`
C shell superuser on UNIX and Linux systems	`machine_name#`
Bourne shell and Korn shell on UNIX and Linux systems	`$`
Bourne shell and Korn shell superuser on UNIX and Linux systems	`#`
Microsoft Windows command line	`C:\`

Symbol Conventions

The following table explains symbols that might be used in this book.

TABLE 3 Symbol Conventions

Symbol	Description	Example	Meaning
`[ ]`	Contains optional arguments and command options.	`ls [-l]`	The `-l` option is not required.
`{ | }`	Contains a set of choices for a required command option.	`-d {y|n}`	The `-d` option requires that you use either the `y` argument or the `n` argument.

TABLE 3 Symbol Conventions *(Continued)*

Symbol	Description	Example	Meaning
`${ }`	Indicates a variable reference.	`${com.sun.javaRoot}`	References the value of the `com.sun.javaRoot` variable.
-	Joins simultaneous multiple keystrokes.	Control-A	Press the Control key while you press the A key.
+	Joins consecutive multiple keystrokes.	Ctrl+A+N	Press the Control key, release it, and then press the subsequent keys.
→	Indicates menu item selection in a graphical user interface.	File → New → Templates	From the File menu, choose New. From the New submenu, choose Templates.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Searching Sun Product Documentation

Besides searching Sun product documentation from the docs.sun.com℠ web site, you can use a search engine by typing the following syntax in the search field:

search-term `site:docs.sun.com`

For example, to search for "broker," type the following:

```
broker site:docs.sun.com
```

To include other Sun web sites in your search (for example, java.sun.com, www.sun.com, and developers.sun.com), use `sun.com` in place of `docs.sun.com` in the search field.

Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 819-3875.

A

abstract schema (n.) The part of an entity bean's deployment descriptor that defines the bean's persistent fields and relationships. See entity bean, persistence. See also schema.

abstract schema name (n.) A logical name that is referenced in EJB QL queries.

access control (1) (n.) The means of securing a server by controlling access to the server.

(2) (n.) The methods by which interactions with resources are limited to collections of users or programs for the purpose of enforcing integrity, confidentiality, or availability constraints.

access control entry See ACE.

access control instruction See ACI.

access control list See ACL.

access control rules (n.) Rules specifying user permissions for a given set of directory entries or attributes.

access domain (n.) A domain that limits access to certain Messaging Server operations from within a specified domain. For example, an access domain can be used to limit where mail for an account can be collected.

accessor (n.) A connector layer that interfaces directly with a directory source over protocols such as LDAP. Identity Synchronization for Windows has separate accessor implementations for Directory Server, Active Directory, and Windows NT. The accessor is often referenced in log messages about an action.

access rights (n.) Access rights specify the level of access control granted or denied. Access rights are related to the type of operation that can be performed on the directory. The following rights can be granted or denied: read, write, add, delete, search, compare, selfwrite, proxy, and all.

account (n.) Information that defines a specific user or user group. This information includes the user name or group name, valid email address or addresses, and how and where email is delivered.

account inactivation (n.) The disabling of a single user account, or set of accounts, so that all authentication attempts are automatically rejected.

ACE (access control entry) (1) (n.) A single item of information from an access control list. Also called access control information.

(2) (n.) A hierarchy of rules that the web server uses to evaluate incoming access requests.

(3) (n.) A string that provides access control for calendars, calendar properties, and calendar components such as events and tasks.

ACI (access control instruction) (n.) An instruction that grants or denies permissions to entries in the directory.

ACID (adj.) The acronym for the four properties guaranteed by a transaction: atomicity, consistency, isolation, and durability.

ACL (access control list) (1) (n.) The mechanism for controlling access to your directory. In Directory Server, an ACL is an ACI attribute in a directory entry.

(2) (n.) A collection of ACEs. An ACL is a mechanism for defining which users have access to your server. You can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users and groups.

(3) (n.) A set of ACE strings that collectively provide access control for calendars, calendar properties, and calendar components such as events and tasks.

(4) (n.) A set of data associated with a directory that defines the permissions that users, groups or users and groups have for accessing the directory. An ACL is composed of one or more ACE strings.

account federation See identity federation.

accumulated patch (n.) A patch which combines the fixes from a previous patch (or patches), any previous versions of the same patch and the current set of fixes being released.

activation (n.) The process of transferring an enterprise bean's state from secondary storage to memory. See also passivation.

active boot environment (n.) The environment that is currently up and running.

active node (n.) An HADB node that contains session data. If an active node fails, a spare node copies data from the mirror node and becomes active. See also HADB node, spare node, mirror node, and data redundancy unit.

address (n.) Information in an email message that determines where and how the message must be sent. Addresses are found both in message headers and in message envelopes. Envelope addresses determine how the message gets routed and delivered. Header addresses are present merely for display purposes.

address handling (n.) The actions performed by the MTA to detect errors in addressing, to rewrite addresses if necessary, and to match addresses to recipients.

addressing protocol (n.) The addressing rules that make email possible. RFC 822 is the most widely used protocol on the Internet and the protocol supported by Messaging Server. Other protocols include X.400 and UUCP.

address token (n.) The address element of a rewrite rule pattern.

admin console (n.) The set of browser-based forms used to configure, administer, monitor, maintain, and troubleshoot a Java™ Enterprise System server and its components.

(n.) The administrator's Directory Server Access Management Edition GUI interface to Portal Server 6.0.

administered object (n.) A pre-configured Java Enterprise System object (a connection factory or a destination) created by an administrator for use by one or more JMS clients.

The use of administered objects isolates Java Message Service (JMS) clients from the proprietary aspects of a provider. These objects are placed in a Java Naming and Directory Interface™ (JNDI) namespace by an administrator and are accessed by JMS clients using JNDI lookups.

administration console See admin console.

administration domain See domain.

administration interface See admin console.

administration node (n.) A Web Server node that can communicate with the remote administration server. Each node in a cluster or server farm has an administration server or administration node running on it. Of these nodes, one is configured to be the master server, referred to as the administration server, and the rest are configured to be slave servers, referred to as administration nodes.

administration privileges (n.) A set of privileges that define a user's administrative role.

administration server (n.) A special server that provides the administrative functions of a Java Enterprise System component product.

administration server administrator (n.) A user who has administrative privileges to start or stop a server even when there is no Java Enterprise System Directory Server connection. The administration server administrator has restricted server tasks (typically only Restart Server and Stop Server) for all servers in a local server group. When an administration server is installed, this administrator\qs entry is automatically created locally. This administrator is not a user in the user directory.

administrative domain See domain.

administrator (n.) A user with a defined set of administrative privileges. See also configuration administrator, Directory Manager, administration server administrator, server administrator family group administrator, mail list owner.

admpw (n.) The user name and password file for the Sun Enterprise™ Administrator Server superuser.

adoption scenario An overall reason for deploying Java Enterprise System software, characterizing the software system you start with and the goal you are trying to achieve. There are four basic Java Enterprise System adoption scenarios: new system, replacement, extension, and upgrade.

affiliation (n.) An affiliation is a group of providers formed without regard to their particular authentication domain. It is formed and maintained by an affiliation owner. An affiliation document describes a group of providers collectively identified by their providerID. Members of an affiliation may invoke services either as a member of the affiliation (by virtue of their Affiliation ID) or individually (by virtue of their Provider ID).

agent (1) (n.) Software that runs the network-management software in a network device, such as a router, host, or X terminal. See also intelligent agent, node agent.

(2) (n.) In Identity Synchronization for Windows, an agent is a connector component that interfaces with Message Queue and translates attributes between their Directory Server names and Windows names. The agent is often referenced in log messages about an action.

alarm event (n.) An event generated and sent by the Calendar Server ENS. When an alarm event occurs, a message reminder is sent to specific recipients.

alert (n.) Time-critical messages that users instantly receive in a pop-up window. The sender knows who has received the message and is notified that the message is read when the alert is either closed or clicked, as long as the "Show message status" option was used. If the alert message requires a response, right clicking on the alert brings up a contextual menu with an option to Chat with Sender.

alias file (n.) A file used to set aliases not set in a directory, such as the postmaster alias.

aliasing (n.) Substituting one item for another in the Java Enterprise System Portal Server Search Engine which uses aliasing when importing resource descriptions from another Search Engine that has a different schema.

All IDs threshold (n.) A size limit that is globally applied to every index managed by the Java Enterprise System Directory Server. When the size of an entry ID list reaches this limit, the server replaces that entry ID list with an All IDs token.

All IDs token (n.) A mechanism that causes the server to assume that all directory entries match the index key. In effect, the All IDs token causes the Java Enterprise System Directory Server to perform an unindexed search to match the index key.

allowed attributes (n.) Optional attributes that can be present in entries using a particular object class. See also attribute, required attributes.

Allow filter (n.) A Java Enterprise System Messaging Server access-control rule that identifies clients that are to be allowed access to one or more POP, IMAP, or HTTP services. See also deny filter.

alternate address (n.) A secondary address for an account, generally a variation on the primary address. In some cases, it is convenient to have more than one address for a single account.

alternate root (n.) The location of the `root` file system on a client on which a package is installed. The alternate root is normally supplied by using `pkgadd -R`.

AML (abstract markup language) (n.) A mobile device markup language that is independent of specific vendors or models.

anonymous access (1) (n.) Accessing a resource without authentication.

(2) (n.) Access, when granted, that allows anyone to access directory information without providing credentials and regardless of the conditions of the bind.

API (application programming interface) (1) (n.) A set of instructions that a computer program can use to communicate with other software or hardware that is designed to interpret that API.

(2) (n.) A set of calling conventions or instructions defining how programs invoke services in existing software packages.

APOP (authenticated post office protocol) (n.) Similar to POP, but instead of using a plaintext password for authentication, APOP uses an encoding of the password together with a challenge string.

applet container (n.) A container that includes support for the applet programming model.

application assembler (n.) A person who combines J2EE™ component*s* and module*s* into deployable application units.

application client (n.) A first-tier J2EE client component that executes in its own Java virtual machine. Application clients have access to some J2EE platform APIs.

application client container (n.) A container that supports application client components. See container.

application client module (n.) A software unit that consists of one or more classes and an application client deployment descriptor.

application component See component.

application component provider (n.) A vendor that provides the Java classes that implement components' methods, JSP page definitions, and any required deployment descriptors.

application configuration resource file (n.) An XML file used to configure resources for a JavaServer Faces application, to define navigation rules for the application, and to register converters, validators, listeners, renderers, and components with the application.

Application Server (n.) The application server product included in Sun Java Enterprise System.

application server (n.) A software platform upon which business applications are run. Application servers typically provide high-level services to applications, such as component life cycle, location, and distribution and transactional resource access.

application service (n.) A component or component assembly that performs business logic on behalf of multiple clients and must therefore be a multithreaded process. An application service can also be a component or component assembly encapsulated as a web service or a stand-alone content server.

application tier (n.) A conceptual division of a J2EE application:

client tier: The user interface. End users interact with client software (such as a web browser) to use the application.

server tier: The business logic and presentation logic that make up your application, defined in the application's components.

data tier: The data access logic that enables your application to interact with a data source.

approximate index (n.) An index that allows for efficient approximate or "sounds-like" searches across the directory information tree.

architecture A design that shows the logical and physical building blocks of a distributed application (or some other software system) and their relationships to one another. In the case of a distributed enterprise application, the architectural design generally includes both the application's logical architecture and deployment architecture

archiving (n.) The process of saving the state of an object and restoring it.

A record (n.) A type of DNS record containing a host name and its associated IP address. An A record is used by messaging servers on the Internet to route email. See also domain name system, MX record.

`asant` (n.) A build tool, based on Apache Ant, that can be extended using Java classes. The configuration files are XML-based, calling out a target tree where various tasks get executed. See also build file.

assembly (n.) The process of combining discrete components of an application into a single unit that can be deployed. See also deployment.

asynchronous communication (n.) A mode of communication in which the sender of a message need not wait for the sending method to return before the sender continues with other work.

attribute (1) (n.) A name-value pair in a request object that can be set by a servlet. Also a name-value pair predefined in a DTD file that modifies an element in an XML file. Contrast with property. See also parameter. More generally, an attribute is a unit of metadata.

(2) (n.) A name-value pair that holds descriptive information about an entry. Attributes have a type (name) and a set of values. An attribute type also specifies the syntax for the kind of information that can be stored as values of attributes of that type.

(3) (n.) Defines the parameters that a Java Enterprise System Directory Server Access Management Edition service provides to an organization. The attributes that make up a Java Enterprise System Directory Server Access Management Edition service are classified as one of the following: Dynamic, Policy, User, Organization, or Global. Using these types to subdivide the attributes in each service allows for a more consistent arrangement of the service schema and easier management of the service parameters.

(4) (n.) In the Application Server, a name-value pair that is part of the built-in server configuration. Contrast with property.

attribute provider (n.) An attribute provider is a web service that hosts attribute data.

attribute list See optional attribute list and required attribute list.

auditing (n.) The method or methods by which significant events are recorded for subsequent examination, typically in error or security breach situations.

AUTH

(n.) An SMTP command enabling an SMTP client to specify an authentication method to the server, perform an authentication protocol exchange, and, if necessary, negotiate a security layer for subsequent protocol interactions.

authenticating Directory Server

(n.) In PTA, the authenticating Java Enterprise System Directory Server contains the authentication credentials of the requesting client. A PTA-enabled user directory passes through bind requests to the authenticating directory, which verifies the bind credentials of the requesting client.

authentication

(1) (n.) The process that verifies the identity of a user, device, or other entity in a computer system, usually as a prerequisite to allowing access to resources in a system. The Java servlet specification requires three types of authentication (basic, form-based, and mutual) and supports digest authentication. In private and public computer networks, including the Internet, authentication is commonly done through the use of login passwords. Knowledge of the password is assumed to guarantee that the user is authentic.See also basic authentication, form-based authentication, mutual authentication, and digest authentication.

(2) (n.) The process of proving the identity of the client user to the Java Enterprise System Directory Server. Users must provide a bind DN and either the corresponding password or certificate in order to be granted access to the directory. Java Enterprise System Directory Server allows the user to perform functions or access files and directories based on the permissions granted to that user by the directory administrator. See also server authentication.

authentication certificate

(n.) A digital file sent from server to client or client to server to verify and authenticate the other party. The certificate ensures the authenticity of its holder, the client or server. Certificates are not transferable.

authentication domain

(n.) A group of service providers with at least one identity provider that agrees to exchange user authentication information using the Liberty Alliance Project (LAP). Once a circle of trust is established, single sign-on authentication is enabled between all the providers. Also called a circle of trust.

authorization

(n.) The process of determining whether a principal can use a service, which objects the principal is allowed to access, and the type of access that is allowed for each object. Authorization depends on the determination of whether the principal associated with a request through authentication is in a given security role. A security role is a logical grouping of users defined by the person who assembles the application. A deployer maps security roles to security identities. Security identities may be principals or groups in the operational environment.

authorization constraint

(n.) An authorization rule that determines who is permitted to access a Web resource collection.

autoreply option file

(n.) A file used for setting options for email autoreply, such as vacation notices.

AutoReply utility (n.) A utility that automatically responds to messages sent to accounts with the AutoReply feature activated. Every account in Java Enterprise System Messaging Server can be configured to automatically reply to incoming messages.

availability service (n.) The Application Server feature for enabling high availability on the server instance, web container, EJB container, and also for RMI/IIOP requests.

B

B2B (adj.) Business-to-business.

backbone (n.) The primary connectivity mechanism of a distributed system. All systems that have connectivity to an intermediate system on the backbone are connected to each other. A backbone does not prevent you from setting up systems to bypass the backbone for reasons of cost, performance, or security.

back-end server (n.) In the context of Java Enterprise System Messaging Server, an email server whose only function is to store and retrieve email messages. Also called a message store server.

backing bean (n.) A JavaBeans component that corresponds to a JSP page that includes JavaServer Faces components. The backing bean defines properties for the components on the page and methods that perform processing for the component. This processing includes event handling, validation, and processing associated with navigation.

backout (n.) The removal of a software change (a patch, for example), which results in returning the system to its previous state.

back up (v.) To copy the contents of folders from the message store to a backup device. See also restore.

backup store (n.) A repository for data, typically a file system or database. A backup store can be monitored by a background thread (sweeper thread) to remove unwanted entries.

banner (n.) A text string displayed by a service such as IMAP when a client first connects to it.

base DN (base distinguished name) (n.) An entry in the DIT. A search operation can be performed on the entry identified by the base DN, the entries that are immediately subordinate to the base DN, or to the entry and all entries below the base DN in the DIT.

basic authentication

(n.) An authentication mechanism in which a Web server authenticates an entity by means of a user name and password obtained using the Web application's built-in authentication mechanism.

bean-managed persistence

(n.) The mechanism whereby data transfer between an entity bean's variables and a resource manager is managed by the entity bean. The data access logic is typically provided by a developer using Java™ Database Connectivity (JDBC™) software or other data access technologies. See also container-managed persistence.

bean-managed transaction

(n.) Transaction demarcation for an enterprise bean that is controlled programmatically by the developer. See also container-managed transaction.

Berkeley DB

(Berkeley database) (n.) A transactional database store intended for high-concurrency read-write workloads and for applications that require transactions and recoverability. Java Enterprise System Messaging Server uses Berkeley databases for numerous purposes.

binary entity

(n.) See unparsed entity.

bind DN

(bind distinguished name) (n.) Distinguished name used to authenticate to a Java Enterprise System Directory Server in the bind request.

binding

(1) (v.) For XML files, generating the code needed to process a well-defined portion of XML data.

(2) (v.) For JavaServer Faces technology, wiring UI components to back-end data sources such as backing bean properties.

bind rule

(n.) In the context of access control, the bind rule specifies the credentials and conditions that a particular user or client must satisfy in order to get access to directory information.

BLOB

(binary large object) (n.) A data type used to store and retrieve complex object fields. BLOBs are binary or serializable objects, such as pictures, that translate into large byte arrays, which are then serialized into container-managed persistence fields.

BMP

See bean-managed persistence.

BMT

See bean-managed transaction.

body

(n.) One part of an email message. Although headers and envelopes must follow a standard format, the body of the message has a content determined by the sender. The body can contain text, graphics, or multimedia. Structured bodies follow the MIME standard.

BPEL

(business process execution language) (n.) A business process language that extends web services for interacting processes. BPEL processes are expressed in XML notation.

broker (n.) The Message Queue entity that manages Java Message Service (JMS) API message routing, delivery, persistence, security, and logging. Provides an interface that allows an administrator to monitor and tune performance and resource use.

browsing (n.) Within Java Enterprise System Portal Server, refers to looking through the categorical divisions of the resources in a Search database.

browsing index See virtual list view index.

build file (n.) The XML file that contains one or more `asant` targets. A target is a set of Apache Ant tasks you want to be executed. When starting `asant`, you can select which targets you want to have executed. When no target is given, the project's default target is executed. See also `asant`.

building module (n.) A hardware or software construct with limited or no dependencies on shared services. A specific configuration that provides optimum performance and horizontal scalability.

business logic (n.) The code that implements the essential functionality of an application rather than data integration or presentation logic. In EJB technology, this logic is implemented by the methods of an enterprise bean.

business method (n.) A method of an enterprise bean that implements the business logic or rules of an application.

business service An application component or component assembly that performs business logic on behalf of multiple clients (and is therefore a multi-threaded process). A business service can also be an assembly of distributed components encapsulated as a web service, or it can be a standalone server.

C

CA (1) (certificate authority) (n.) See certificate authority.

(2) (connector architecture) (n.) See connector architecture.

cache (n.) A copy of original data that is stored locally. Cached data does not have to be retrieved from a remote server again when requested.

Cache Control Directive (n.) A way for Java Enterprise System Application Server to control what information is cached by a proxy server. Using cache control directives, you override the default caching of the proxy to protect sensitive information from being cached and perhaps retrieved later. For these directives to work, the proxy server must comply with HTTP 1.1.

cached rowset (n.) An object that permits you to retrieve data from a data source and then detach from the data source while you examine and modify the data. A cached row set keeps track both of the original data retrieved and any changes made to the data by your application. If the application attempts to update the original data source, the row set is reconnected to the data source, and only those rows that have changed are merged back into the database.

calendar access protocol See CAP.

Calendar Express (n.) A web-based calendar client program that provides access to the Calendar Server for end users.

calendar group (n.) A collection of several calendars to help a user manage more than one calendar.

calendar ID (n.) A unique identifier associated with a calendar in the Java Enterprise System Calendar Server database. Also known as `calid`.

calendar lookup database See CLD.

Calendar Server application programming interface See CSAPI.

calendar user agent See CUA.

callable statement (n.) A class that encapsulates a database procedure or function call for databases that support returning result sets from stored procedures.

callback method (n.) A component method called by the container to notify the component of important events in its life cycle.

caller (n.) Same as caller principal.

caller principal (n.) The principal that identifies the invoker of the enterprise bean method.

CAP (calendar access protocol) (n.) A standard Internet protocol for calendaring based on requirements identified by the Internet Engineering Task Force (IETF).

capability (n.) A string provided to clients that defines the functionality available in a given IMAP service.

cascading deletion (n.) A deletion that triggers another deletion. A cascading deletion can be specified for an entity bean that has container-managed persistence.

cascading replication (n.) In a cascading replication scenario, one server, often called the hub supplier, acts both as a consumer and a supplier for a particular replica. The server holds a read-only replica and maintains a change log. The server receives updates from the supplier server that holds the master copy of the data and, in turn, supplies those updates to the consumer.

catalog See index.

cataloging See indexing.

category (n.) A logical grouping of resources in the Search database. Collectively, a set of categories is sometimes called a taxonomy.

CCPP (composite capability and preference profiles) (n.) For Portal Server Mobile Access software, a specification that is used for the User Agent Profile and preconfigured data for client detection. The CCPP specification describes the capabilities of devices and user preferences.

`CDATA` (n.) A predefined XML tag for character data that means "don't interpret these characters," as opposed to parsed character data (`PCDATA`), in which the normal rules of XML syntax apply. `CDATA` sections are typically used to show examples of XML syntax. See also `PCDATA`.

central logger (n.) A Core component that manages all of the central logs, which are an aggregation of every connector's audit and error logs. Administrators can monitor the health of an entire Identity Synchronization for Windows installation by monitoring these logs. You can view the central

logs directly or from the Identity Synchronization for Windows Console. By default, the central logs are available on the machine where Core was installed under the <*install-root*\>/logs/central/ subdirectory.

certificate (1) (n.) An electronic document used to identify an Instant Messaging Server and associated with a public key. Java Enterprise System Instant Messaging Server supports the exchange of certificates between Instant Messaging servers. The certificate exchange is transparent to individual users.

(2) (n.) Digital data that specifies the name of an individual, company, or other entity and certifies that the public key included in the certificate belongs to that entity. Both clients and servers can have certificates.

(3) (n.) A certificate strongly associates the public key of a user or CA with the identity, typically a distinguished name, of that user or CA. The certificate is digitally signed by a CA, and can be validated during an SSL connection setup to obtain the public key of the other end of the connection. X.509 certificates are stored within the directory in the `caCertificate;binary` or `userCertificate;binary` attributes.

certificate authority (1) (n.) An internal or third-party trusted organization that issues public key certificates used for encrypted transactions and provides identification to the bearer.

(2) (n.) An authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a PKI, a CA checks with a registration authority to verify information provided by the requestor of a digital certificate. If the registration authority verifies the requestor's information, the CA can then issue a certificate. See also PKI.

certificate-based authentication (n.) Identification of a user from a digital certificate submitted by the client. See also password authentication.

certificate database (n.) A file that contains a server's digital certificate or certificates. Also called a certificate file.

certificate name (n.) The name that identifies a certificate and its owner.

certificate revocation list See CRL.

CGI (common gateway interface) (n.) An interface by which external programs communicate with the HTTP server. Programs that are written to use CGI are called CGI programs or CGI scripts. CGI programs handle forms or parse output the server does not normally handle or parse.

cHTML (n.) A simplified version of HTML suitable for mobile devices.

change log (n.) A change log is a record of the modifications that have occurred on a replica. The supplier server then replays these modifications on the replicas stored on consumer servers or on other masters, in the case of multimaster replication. Note that this is not the same as the retro changelog, which is not used for replication.

channel (1) (n.) The fundamental MTA component that processes a message. A channel represents a connection with another computer system or group of systems. Each channel consists of one or more channel programs and an outgoing message queue for storing messages that are destined to be sent to one or more of the systems associated with the channel. See also channel block, channel host table, channel program.

(2) (n.) In the Java Enterprise System Portal Server Desktop, a channel consists of a provider and configuration. Channels generate content that can consist of markup fragments, a frameset, an HTML page, and so on. Channel content is often aggregated with other channel content to form a Portal Desktop.

channel block (n.) A single channel definition. See also channel host table.

channel host table (n.) The collective set of channel definitions. See also channel block

channel program (n.) Part of a channel that transmits messages to remote systems and deletes messages from the queue after they are sent and accepts messages from remote systems placing them in the appropriate channel queues. See also master channel program, slave channel program.

character type (n.) An attribute that distinguishes alphabetic characters from numeric or other characters and the mapping of uppercase to lowercase letters.

chat (n.) Instant Messaging's version of instant messaging. Chat is a real-time conversation capability. Chat sessions are held either in chat rooms created on an as-needed basis or in pre-established conference rooms.

checkpoint (n.) A predefined point in the life cycle of a stateful session bean at which the bean's state is saved in a persistent store in case an Application Server instance fails.

child (1) (n.) A category that is a subcategory of another category. See also category.

(2) (n.) An element in an XML file that is contained within another element, referred to as the parent. See also parent.

chroot (n.) An additional root directory you can create to limit the server to specific directories. You would use this feature to safeguard an unprotected server.

cipher (n.) A cipher is a cryptographic algorithm (a mathematical function) used for encryption or decryption.

ciphertext (n.) Encrypted information that cannot be read by anyone without the proper key to decrypt the information.

circle of trust (n.) See authentication domain.

CKL (compromised key list) (n.) A list of key information about users who have compromised keys. The certificate authority also provides this list. See also CRL.

classic CoS (n.) Identifies the template entry by its DN and the value of one of the target entry\qs attributes.

classification rules (n.) A set of rules used to assign resources to a category or to several categories.

class loader (n.) A Java™ technology-based component responsible for loading Java classes according to specific rules.

class of service See CoS.

CLD (Calendar Lookup Database) (n.) A plug-in that determines the physical location of a calendar when the calendar database is distributed over two or more back-end servers. Calendar Server provides the LDAP CLD plug-in and the algorithmic CLD plug-in.

cleartext (n.) Unencrypted text.

client-certificate authentication (n.) An authentication mechanism that uses HTTP over SSL, in which the server and, optionally, the client authenticate each other with a public key certificate that conforms to a standard that is defined by X.509 Public Key Infrastructure. See also authentication, certificate authority.

client contract (n.) A contract that determines the communication rules between a client and the EJB™ container, establishes a uniform development model for applications that use enterprise beans, and guarantees greater reuse of beans by standardizing the relationship with the client.

client conditional properties (n.) Properties of Portal Server Mobile Access client types that enable administrators to specify properties for a channel or container channel for a given client.

client database (n.) For Portal Server Mobile Access, a database that consists of an internal and an external library. The internal library contains all default mobile device data definitions. The external library contains customized client data definitions that override definitions in the internal library.

client detection (n.) An Access Manager process which determines the capabilities and characteristics of each mobile device that accesses the portal.

Client Editor (n.) An Access Manager interface that enables you to create a client type and to manage client properties. The Client Editor interface is accessible from the Access Manager console.

client identifier (n.) An identifier that associates a connection and its objects with a state maintained by the Java Enterprise System message server on behalf of the client.

Client Manager (n.) An Access Manager interface accessible from the console that enables you to manage client types and properties.

client profile (n.) An Access Manager profile that identifies each client.

***client runtime** See Java Enterprise System client runtime.

client-server model (n.) A computing model in which networked computers provide specific services to other client computers. Examples include the name-server and name-resolver paradigm of the DNS and file-server/file-client relationships such as NFS and diskless hosts.

***client type** (n.) An entry in the Access Manager client database.

clientType (n.) A property which refers to a name that provides a unique index for Access Manager client data.

cluster (1) (n.) A group of servers, brokers, or nodes connected by a high-speed network that work together as if they were one server, broker, or node. If a server, broker, or node in the cluster fails, its services can failover to an operational one. See also broker, failover, node, server.

CMP See container-managed persistence.

CMR See container-managed relationship.

CMT See container-managed transaction.

cn See common name attribute.

CNAME record (n.) A type of DNS record that maps a domain name alias to a domain name.

collation order (n.) Language and cultural-specific information about how the characters of a given language are to be sorted. This information might include the sequence of letters in the alphabet or how to compare letters with accents to letters without accents.

collection (n.) A database that contains information about documents, such as a word list and file properties. Collections are used by the search function to retrieve documents matching specified search criteria.

colocation (n.) The property of being on the same node. This concept is used during cluster configuration to improve performance.

colocate (v.) To position a component in the same memory space as a related component in order to avoid remote procedure calls and improve performance.

column (n.) A field in a database table.

comm_dssetup.pl (n.) A Directory Server preparation tool that makes an existing Directory Server ready for use by a Messaging Server.

comment (n.) In an XML document, text that is ignored unless the parser is specifically told to recognize it.

comment character (n.) A character at the beginning of a line that turns the line into a nonexecutable comment.

commit (1) (v.) To complete a transaction by sending the required commands to the database or other resource. See also rollback, transaction.

(2) (n.) The point in a transaction when all updates to any resources involved in the transaction are made permanent.

common domain (n.) In a circle of trust having more than one identity provider, service providers need a way to determine which identity provider a principal uses. Because this function must work across any number of domain name system (DNS) domains, the Liberty approach is to create a domain common to all identity and service providers in the circle. This predetermined domain is known as the common domain. Within the common domain, when a principal has been authenticated to a service provider, the identity provider writes a common domain cookie that stores the principal's identity provider. Now, when the principal attempts to access another service provider within the circle, the service provider reads the common domain cookie and the request can be forwarded to the correct identity provider.

common log file format (n.) The format used by the server for entering information into the access logs. The format is the same among all major servers, including the Web Server.

common name attribute (n.) The cn attribute that identifies the person or object defined by the entry in an LDAP directory.

Communication Services (n.) A comprehensive messaging solution that enables the delivery of the integrated email, calendar, instant messaging, and presence information to enterprise customers. The Communication Services core solution consists of Messaging Server, Calendar Server and Instant Messaging Server.

Communications Express (n.) Software that provides an integrated web-based communication and collaboration client that caters to the needs of enterprise users for accessing email, calendar, and address book information.

Compass (n.) A search engine service that provided the search capability for Portal Server 3.0. The search engine has been incorporated into the core of Portal Server 6.0. See Search Engine.

Compass Server (n.) Server technology used to facilitate user access to network resources typically used with Portal Server 3.0. Portal Server 6.0 contains a tightly integrated search engine which provides the functionality that Compass Server provided with Portal Server 3.0.

component (1) (n.) One of the system component*s* included in Java Enterprise System.

(2) (n.) A unit of software logic from which distributed applications are built. An application component is custom developed and usually conforms to a distributed component model (such as CORBA and the J2EE platform) and performs some specific computing function. These components, singly or combined, provide business service*s* and can be encapsulated as web service*s*.

(3) (n.) See J2EE component.

component contract (n.) The contract between a J2EE component and its container. The contract includes life-cycle management of the component, a context interface that the instance uses to obtain various information and services from its container, and a list of services that every container must provide for its components.

component-managed sign-on (n.) A mechanism whereby security information needed for signing on to a resource is provided by an application component.

component product descriptor file (n.) A file containing metadata for a given component product (usually in XML format).

component state (n.) A set of attributes that describe a calendar event such as a meeting. In WCAP, the `compstate` parameter allows fetch commands to return events by component state. For example, `compstate` might be `REPLY-DECLINED` (attendee has declined a meeting) or `REQUEST_NEEDS-ACTION` (attendee has not taken action on a meeting yet).

compromised key list See CKL.

computed attribute (n.) An attribute that are not stored with the entry itself but are returned to the client application along with normal attributes in operation results.

conference room (n.) A pre-established chat room configured by an administrator or other user with `sysRoomsAdd` privilege. The administrator or other user with `sysRoomsAdd` privilege can determine which users can view and access conference rooms.

configuration (n.) A collection of settings for tuning a server or providing metadata for an application. Normally, the configuration for a specific application is kept in the application's deployment descriptor file. See also admin console, deployment descriptor.

configuration administrator (n.) The person who has administrative privileges to manage servers and configuration directory data in the entire server software topology. The configuration administrator has unrestricted access to all resources in the entire server software topology. This is the only administrator who can assign server access to other administrators. The configuration administrator initially manages administrative configuration until the administrator's group and its members are in place.

Configuration Directory Server (n.) A Java Enterprise System Directory Server that maintains configuration information for a server or set of servers.

configuration file (n.) A file that contains the configuration parameters for a server, application, or software component.

conflict (n.) A situation that arises when changes are made to the same directory data on different directory servers before replication can synchronize the data between the servers. When the servers do synchronize, they detect that their copies are inconsistent and might resolve the conflict or log an error.

conflict resolution (n.) Deterministic procedures used to resolve change information. For more information, see the Java Enterprise System Directory Server Administration Guide.

congestion thresholds (n.) A disk space limit set by the system administrator that prevents the database from becoming overloaded by restricting new operations when system resources are insufficient.

connection (1) (n.) For a resource manager, an object that represents a session with a resource manager.

(2) (n.)An active connection to a Java Enterprise System message server. The connection can be a queue connection or a topic connection.

connection factory (1) (n.) For a resource manager, an object used for creating a resource manager connection.

(2) (n.) An object used to create Java Message Service (JMS) connections (`TopicConnection` or `QueueConnection`) which allow application code to make use of the provided JMS implementation. Application code uses the Java Naming and Directory Interface™ (JNDI) service to locate connection factory objects using a JNDI name.

connection handler (n.) Used by Directory Proxy Server to distribute incoming client requests to data views. Connections are assigned to connection handlers according to criteria such as incoming IP address or domain name. When processing connections, connection handlers refer to connection policies.

connection policy (n.) A policy rule for making decisions about how to process an operation routed by a Directory Proxy Server connection handler. Resource limits policies limit the resources allocated to connections, requests, and referrals. Request filtering policies provide access control for data.

connection pool (n.)A group of connections. Allows highly efficient access to a database by caching and reusing physical connections, thus avoiding connection overhead and allowing a small number of connections to be shared between a large number of threads. See also JDBC connection pool.

connector (n.) A standard extension mechanism for containers to provide connectivity to an EIS. A connector is specific to an EIS and consists of a resource adapter and application development tools for EIS connectivity. The resource adapter is plugged in to a container through its support for system-level contracts defined in the connector architecture. See also resource adapter.

connector architecture (n.) An architecture for the integration of J2EE™ applications with an EIS. There are two parts to this architecture: an EIS vendor-provided resource adapter and a J2EE server that allows this resource adapter to plug in. This architecture defines a set of contracts that a resource adapter has to support to plug in to a J2EE server, for example, transactions, security and resource management.

Connector for Microsoft Outlook (n.) A plug-in that enables Microsoft Outlook to be used as a desktop client with Sun Java Enterprise System.

console See admin console.

consume (v.) To receive a message taken from a destination by a message consumer.

consumer (1) (n.) A server containing replicated directory trees or subtrees from a supplier server.

(2) (n.) An object (MessageConsumer) created by a session that is used for receiving messages from a destination. In the point-to-point delivery model, the consumer is a receiver or browser (QueueReceiver or QueueBrowser). In the publish/subscribe delivery model, the consumer is a subscriber (TopicSubscriber).

consumer directory server (1) (n.) A read-only directory server that refers all add, modify, and delete operations to master directory servers.

(2) (n.) Any directory server that receives changes from another directory server. See supplier directory server.

contact (n.) The userID (name) of a user or LDAP group with whom you send and receive instant messages. You add contacts to your personalized contact groups so that you can monitor their online status. Also known as buddy in other instant messaging environments.

contact group (n.) A list of contacts that a user maintains. The actual list is stored on the Instant Messaging Server. You can create contact groups to keep track of people in a logical way.

contact list (n.) In Java Enterprise System Instant Messaging, the list of all of your contact groups.

container (1) (n.) Provides life-cycle management, security, deployment, and runtime services to a specific type of J2EE component. The Application Server provides containers for all types of J2EE components. See also component.

(2) (n.) In Java Enterprise System Portal Server 6.0, a container is a channel that primarily generates its content by aggregating the content of its child channels. In Java Enterprise System Directory Server Access Management Edition, a container defines a type of organizational object that can contain other Directory Server Access Management Edition objects.

container entry (n.) An entry that represents the top of a subtree in the directory.

container-managed persistence (n.) The mechanism whereby data transfer between an entity bean*'s* variables and a resource manager is managed by the entity bean's container. See also bean-managed persistence.

container-managed relationship (n.) A relationship between fields in a pair of classes where operations on one side of the relationship affect the other side.

container-managed sign-on (n.) A mechanism whereby security information needed for signing on to a resource is supplied by the container.

container-managed transaction (n.) The mechanism whereby transaction demarcation for an enterprise bean is specified declaratively and automatically controlled by the EJB container. An entity bean must use container-managed transactions. See also bean-managed transaction.

content (n.) In an XML document, the part that occurs after the prolog, including the root element and everything it contains.

context attribute (n.) An object bound into the context associated with a servlet.

context root (n.) A name that gets mapped to the document root of a web application.

control descriptor (n.) A set of enterprise bean configuration entries that enable you to specify optional individual property overrides for bean methods, plus enterprise bean transaction and security properties.

controller (n.) An Identity Synchronization for Windows connector component interfaces with the agent and accessor components. The controller performs key synchronization-related tasks such as determining a user's membership in a Synchronization User List, searching for and linking equivalent user entries, and detecting changes to users by comparing current user entries with the previous versions stored in the object cache. The controller is often referenced in log messages about an action.

conversational state (1) (n.) Where the state of an object changes as the result of repeated interactions with the same client. See also persistent state.

(2) (n.) The field values of a session bean plus the transitive closure of the objects reachable from the bean's fields. The transitive closure of a bean is defined in terms of the serialization protocol for the Java programming language, that is, the fields that would be stored by serializing the bean instance.

cookie (n.) A small collection of information that can be transmitted to a calling web browser, then retrieved on each subsequent call from that browser so the server can recognize calls from the same client. Cookies are domain-specific and can take advantage of the same web server security features as other data interchange between your application and the server. Accepting the cookies allows the web page to load more quickly and is not a threat to the security of your machine.

cooperating server (n.) A server that wants to communicate with your server and a server with which your server wants to communicate. Also known as a coserver. Each cooperating server is given a symbolic name, which is a string consisting of letters and digits, for example, `coserver`*n*, where *n* is a number.

CORBA (common object request broker architecture) (n.) A standard, language-independent architecture definition for object-oriented distributed computing specified by the OMG.

core service (n.) One or more key services that define the basic functionality provided by a Java Enterprise System server, as opposed to support services or adjunct services.

CoS (class of service) (n.) A method for sharing attributes between entries.

CoS definition entry (n.) An entry identifies the type of CoS you are using. The entry is stored as an LDAP subentry below the branch it affects.

coserver See cooperating server.

CoSNaming provider (n.) To support a global JNDI name space (accessible to IIOP application clients), Java Enterprise System Application Server includes J2EE based CosNaming provider which supports binding of CORBA references (remote EJB references).

CoSNaming Service (n.) An an IIOP-based naming service.

CoS template entry (n.) An entry which contains a list of the shared attribute values.

CRAM-MD5 (n.) A lightweight standards track authentication mechanism documented in RFC 2195. It provides a fast (albeit somewhat weaker) alternative to TLS (SSL) when only the user's login password needs to be protected from network eavesdroppers.

crawler See robot.

`create` **method** (n.) A method defined in the home interface and invoked by a client to create an enterprise bean.

CRL (certificate revocation list) (n.) A list published by a certificate authority that indicates any certificates that either client users or server users should no longer trust. In this case, the certificate has been revoked. See also CKL.

cronjob (n.) (UNIX only) A task that is executed automatically by the cron daemon at a configured time.

CSAPI (Calendar Server application programming interface) (n.) A programmatic interface that provides the capability to modify or enhance the feature set of the Calendar Server. CSAPI modules are plug-ins that are loaded from the `cal/bin/plugins` directory when the Calendar Server is started.

CSS (1) (Cascading style sheet) (n.) A stylesheet used with HTML and XML documents to add a style to all elements marked with a particular tag, for the direction of browsers or other presentation mechanisms.

CTS (Compatibility test suite) (n.) A suite of compatibility tests for verifying that a J2EE product complies with the J2EE platform specification.

CUA (Calendar user agent) (n.) An application that a calendar client uses to access the Calendar Server.

D

DAP (directory access protocol) (n.) The ISO/ITU-T X.500 protocol that was the basis for LDAP.

data (n.) The contents of an element in an XML stream, generally used when the element does not contain any subelements. When it does, the term content is generally used. When the only text in an XML structure is contained in simple elements and when elements that have subelements have little or no data mixed in, then that structure is often thought of as XML data, as opposed to an XML document.

data access logic (n.) Business logic that involves interacting with a data source.

database (n.) A generic term for relational database management system (RDBMS). A software package that enables the creation and manipulation of large amounts of related, organized data. See also schema.

database connection (n.) A communication link with a database or other data source. Components can create and manipulate several database connections simultaneously to access data.

database wire protocol See data redundancy unit.

data redundancy unit (DRU) (n.) A set of HADB nodes containing half of the active and spare nodes and one complete copy of the data. The HADB is organized into two DRUs, which mirror each other. To ensure fault tolerance, the computers that support one DRU must be completely self-supported with respect to power, processing units, and storage. See also HADB node, active node, spare node, and mirror node.

data service (n.) A web service that supports the query and modification of data regarding an end user. An example of a data service is a web service that hosts and exposes the user's profile information, such as name, address, and phone number.

data source (1) (n.) A handle to a source of data, such as a database. Data sources are registered with the Application Server and then retrieved programmatically in order to establish connections and interact with the data source. A data-source definition specifies how to connect to the source of data.

(2) (n.) A repository accessed by Directory Proxy Server. Repositories include LDAP directories, JDBC-compliant databases, and LDIF flat files.

data source object (n.) A data source object has a set of properties that identify and describe the real world data source that it represents.

data source pool (n.) A set of data sources holding equivalent data. Data source pools provide load balancing and failover management for Directory Proxy Server.

data store (1) (n.) A store that contains directory information, typically for an entire DIT.

(2) (n.) A database where information (durable subscriptions, data about destinations, persistent messages, auditing data) needed by the Message Queue broker is permanently stored.

data view (n.) Uses DN-based routing to route connections from Directory Proxy Server connection handlers to data source pools.

DC tree (domain component tree) (n.) A DIT that mirrors the DNS network syntax. An example of a distinguished name in a DC Tree would be `cn=billbob,dc=bridge,dc=net,o=internet`.

DDP (Document-driven programming) (n.) The use of XML to define applications.

declaration (n.) The very first thing in an XML document, which declares it as XML. The minimal declaration is `<?xml version="1.0"?>`. The declaration is part of the document prolog.

declarative security (n.) Declaring security properties in the component's deployment descriptor and allowing the component's container (for example, a bean's container or a servlet engine) to manage security implicitly. This type of security requires no programmatic control. Opposite of programmatic security. See also container-managed persistence.

declarative transaction See container-managed transaction.

decryption (n.) The process of making encrypted information intelligible. See also encryption.

default calendar (n.) The calendar a user first sees after logging into Calendar Express. The calendar ID of a default calendar is the usually same as the user's user ID. For example, `jdoe@example.com` would have a default calendar named `jdoe`.

default index (n.) A set of indexes that is created for each database instance when Directory Server is installed. When Java Enterprise System Directory Server is installed, a set of default indexes is created for each database instance. For more information, see the Java Enterprise System Directory Server Administration Guide.

defederation (n.) See federation termination.

definition entry See CoS definition entry.

defragmentation (n.) The MIME feature that enables a large message that has been broken into small messages or fragments to be reassembled. A Message Partial Content-Type header field that appears in each of the fragments contains information that helps reassemble the fragments into one message. See also fragmentation.

Delegated Administrator (n.) A set of GUI and CLI interfaces that enable administrators to add users to and modify users and groups of a directory in a hosted domain.

delegated administrator console (n.) A web browser-based software console that allows domain administrators to add and modify users and groups to a hosted domain. Also allows end users to change their password, set message forwarding rules, set vacation rules, and list mail list subscriptions.

delegated administrator for messaging and collaboration (n.) A set of interfaces (GUI and utilities) that allow domain administrators to add and modify users and groups on a hosted domain.

delegated administrator server (n.) A daemon program that handles access control to the directory by hosted domains.

delegation (1) (n.) An object-oriented technique for using the composition of objects as an implementation strategy. One object, which is responsible for the result of an operation, delegates the implementation to another object. For example, a classloader often delegates the loading of some classes to its parent. See also class loader.

delete a message (v.) To mark a message for deletion. The deleted message is not removed from the message store until it is expunged or purged in a separate action by the user. See also purge a message, expunge a message.

delivery See message delivery.

delivery mode (n.) A mode that indicates the reliability of messaging: messages that are guaranteed to be delivered and successfully consumed once and only once (persistent delivery mode) or are guaranteed to be delivered at most once (non-persistent delivery mode).

delivery model (n.) A model by which messages are delivered. The model can be either point-to-point or publish/subscribe. In Java™ Message Service (JMS), separate programming domains exist for each, using specific client runtime objects and specific destination types (queue or topic), as well as a unified programming domain.

delivery policy (n.) A specification that details how a queue is to route messages when more than one message consumer is registered. The policies are single, failover, and round-robin.

delivery status notification (n.) A message giving status information about a message that is en route to a recipient, for example, a message indicating that delivery has been delayed because of network outages.

denial of service attack (n.) A situation where an individual intentionally or inadvertently overwhelms a mail server by flooding it with messages. A server's throughput could be significantly impacted or the server itself could become overloaded and nonfunctional.

deny filter (n.) A Java Enterprise System Messaging Server access-control rule that identifies clients that are to be denied access to one or more of the following services: POP, IMAP, or HTTP. See also Allow filter.

deployer (n.) A person who installs J2EE modules and applications into an operational environment.

deployment (1) (n.) The process whereby software is installed into an operational environment.

(2) (n.) A stage of the Java Enterprise System solution life-cycle process in which a deployment scenario is translated into a deployment design, implemented, prototyped, and rolled out in a production environment. The end product of this process is also referred to as a deployment (or deployed solution).

deployment architecture (n.) A high-level design that depicts the mapping of a logical architecture to a physical computing environment. The physical environment includes the computers in an intranet or Internet environment, the network links between them, and any other physical devices needed to support the software.

deployment descriptor (n.) An XML file provided with each module and application that describes how the applications should be deployed. The deployment descriptor directs a deployment tool to deploy a module or application with specific container options and describes specific configuration requirements that a deployer must resolve. See also metadata.

deployment scenario (n.) A logical architecture for a Java Enterprise System solution and the quality-of-service requirements that the solution must satisfy to meet business needs. The quality-of-service requirements include requirement regarding: performance, availability, security, serviceability, and scalability/latent capacity. A deployment scenario is the starting point for deployment design.

depth (n.) The number of links followed from a site\qs starting point in the Search Engine. When you define a site, you define the number of links the robot can follow away from that point, thereby limiting the depth of the search.

dereference an alias (v.) To specify in a bind or search operation, that a directory service translate an alias distinguished name to the actual distinguished name of an entry.

Desktop See Portal Server Desktop.

destination (n.) The physical location in a Java Enterprise System message server to which produced messages are delivered for routing and subsequent delivery to consumers. This physical destination, a queue or topic, is identified and encapsulated by an administered object. A client uses the administered object to specify the destination for which the client is producing messages and/or from which the client is consuming messages. See also point-to-point delivery model, publish and subscribe delivery model.

destination resource (n.) An object that represents Topic or Queue destinations. Used by applications to read and write to Queues or publish and subscribe to Topics. Application code uses the Java Naming and Directory Interface™ (JNDI) Service to locate Java Message Service (JMS) resource objects using a JNDI Name.

development (n.) A task in the Java Enterprise System solution deployment process, by which the custom components of a deployment architecture are programmed and tested.

device detection See client detection.

device information (n.) Device-specific client data for Portal Server Mobile Access.

DHCP (dynamic host configuration protocol) (n.) An Internet proposed standard protocol that allows a system to dynamically assign an IP address to individual computers on a network. See also IP address.

digest authentication (n.) A type of authentication which allows the user to authenticate without sending the username and password as cleartext. A web application authenticates itself to a web server by sending the server a message digest along with its HTTP request message. The digest is computed by employing a one-way hash algorithm (called MD5) to a concatenation of the HTTP request message and the client's password. The digest is typically much smaller than the HTTP request and doesn't contain the password. The server uses the Digest Authentication plug-in to compare the digest value provided by the client.

DIGEST-MD5 (n.) A lightweight standards track authentication mechanism that is more secure then CRAM-MD5. Documented in RFC 2831 which also provides an option to protect the entire connection without the setup overhead of TLS (SSL).

digital signature (n.) An electronic security mechanism used to authenticate both a message and the signer.

directive (n.) A Search Engine statement that uses a particular format to invoke a function (such as a robot application function) and passes parameters to the function in a parameter block. For example, the following directive invokes the `enumerate-urls` function and passes parameters for `max` and `type`:

```
Enumerate fn=enumerate-urls max=1024 type=text/html
```

directory (n.) A special kind of database optimized for reading data rather than writing data. Most directories are based on LDAP (Lightweight Directory Access Protocol), an industry-standard protocol.

directory access protocol See DAP.

directory context (n.) The point in the directory tree information at which a search begins for entries used to authenticate a user and password for message store access. See also base DN.

directory deployment (n.) In the Application Server, the deployment of an unpackaged J2EE application or module in the form of an exploded directory instead of an archive file.

directory entry (n.) A set of directory attributes and their values identified by a distinguished name. Each entry contains an object class attribute that specifies the kind of object the entry describes and defines the set of attributes it contains.

directory information tree See DIT.

directory lookup (n.) The process of searching the directory for information on a given user or resource based on that user or resource's name or other characteristic.

Directory Manager (1) (n.) A user who has administrative privileges to the directory server database. Access control does not apply to this user (think of the directory manager as the directory\qs superuser).

(2) (n.) The privileged database administrator who is comparable to the root user on UNIX systems. Access control does not apply to the directory manager.

directory schema (n.) The set of rules that defines the data that can be stored in the directory.

Directory Server (n.) The Java Enterprise System version of Lightweight Directory Access Protocol. Every instance of Application Server uses Directory Server to store shared server information, including information about users and groups.

Directory Server Access Management Edition (n.) A set of interfaces that provide user and service management, authentication and single sign-on services, policy management, logging services, debug utility, and client support for Portal Server.

directory server (1) (n.) A server that serves information about people and resources within an organization from a logically centralized repository. See also LDAP and Directory Server Access Management Edition

(2) (n.) The Java Enterprise System directory service based on LDAP.

directory service (n.) A database application designed to manage descriptive, attribute-based information about people and resources within an organization.

Directory Service Control Center (n.) A browser-based GUI for administering Directory Server and Directory Proxy Server.

Directory Service Manager (n.) An LDAP superuser that manages server configuration and data on multiple Directory Servers and Directory Proxy Servers through Directory Service Control Center.

directory synchronization (n.) The process of synchronizing the MTA directory cache with the current directory information stored in the directory service. See also MTA directory cache.

disconnected state (n.) The state in which a mail client connects to the server, makes a cache copy of selected messages, then disconnects from the server.

Dispatcher (n.) The MTA component that handles connection requests for defined TCP ports. The Dispatcher is a multithreaded connection dispatching agent that permits multiple multithreaded servers to share responsibility for a given service. When using the Dispatcher, you can have several multithreaded SMTP server processes running concurrently.

display profile (n.) A set of XML documents used to define and configure providers and channels in Java Enterprise System Portal Server.

distinguished name See DN.

distributable session (n.) A user session that is distributable among all servers in a cluster.

Distributed Authentication UI Server (n.) An Access Manager subcomponent that provides for secure, distributed authentication across two firewalls in an Access Manager deployment. You install the Distributed Authentication UI subcomponent on one or more servers within the non-secure (DMZ) layer of an Access Manager deployment. This subcomponent acts as an authentication interface between end users and the Access Manager instances behind the second firewall, thus eliminating the exposure of the Access Manager service URLs to the end users.

distributed enterprise application (n.) An application whose logic spans a network or Internet environment (the distributed aspect) and whose scope and scale meet the needs of a production environment or service provider (the enterprise aspect). The application's components run in separate runtime environments, usually on different platforms. Typical distributed applications are two-tier (client-server), three-tier (client-middleware-server), and multi-tier (client-multiple middleware-multiple servers).

distributed indexing (n.) The process of assigning different robots in the Search Engine to index different parts of the network. Distributed indexing reduces the load on each robot. A single Search Engine can then gather all the resource descriptions from all the different robots by importing resource descriptions from each.

distributed transaction (n.) A single transaction that can apply to multiple heterogeneous databases that might reside on separate servers.

distribution list See mail list.

distribution list owner See mail list owner.

DIT (directory information tree) (n.) The logical representation of the information stored in the directory. The DIT mirrors the tree model used by most file systems, with the tree\qs root point appearing at the top of the hierarchy.

DN (distinguished name) (n.) String representation of an entry\qs name and location in the directory.

DN attribute (n.) A text string that contains identifying information for an associated user, group, or object.

DNS (domain name system) (n.) The system used by machines on a network to associate IP addresses (such as 00.120.000.168) with host names (such as `www.example.com`). Clients usually use DNS to find the IP addresses of servers they wish to contact. The data in DNS is often augmented in local tables, such as from NIS or the `/etc/hosts` file on UNIX systems. See also IP address.

DNS alias (n.) A host name that the DNS server knows points to a different host. The DNS alias is implemented as a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as `www.example.com` might point to a real machine called `realthing.example.com` where the server currently exists.

DNS database (n.) A database of domain names (host names) and their corresponding IP addresses.

DNS domain (n.) A group of computers whose host names share a common suffix, the domain name. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), for example, `corp.mktng.example.com`. See also domain.

DNS spoofing (n.) A form of network attack in which a DNS server has been subverted to provide false information.

document (1) (n.) A file on the network, most often a web page or word processing document, but also possibly text files, spreadsheets, and so on. A generic term for a resource indexed by the Search Engine.

(2) (n.) An XML structure in which one or more elements contains text intermixed with subelements. See also data.

Document Object Model (DOM) (n.) An API for accessing and manipulating XML documents as tree structures. DOM provides platform-neutral, language-neutral interfaces that enables programs and scripts to dynamically access and modify content and structure in XML documents.

document root (1) (n.) A directory on the server machine that contains files, images, and data that will be displayed to users accessing Java Enterprise System Web Server.

(2) (n.) A directory on the server machine that contains the files, images, and data you want to present to users accessing the server.

(3) (n.) The document root (sometimes called the primary document directory) is the central directory that contains all the virtual server's files you want to make available to remote clients.

document type definition See DTD.

domain (1) (n.) The last part of a fully qualified domain name that identifies the company or organization that owns the domain name (for example, `example.com`, `host.example.com`).

(2) (n.) Resources under the administrative control of a single computer system.

(3) (n.) A set of objects used by Java Message Service (JMS) clients to program JMS messaging operations. Two programming domains exist: one for the point-to-point delivery model and one for the publish/subscribe delivery model.

(4) (n.) A feature within the Sun Java System Application Server that allows different administrative users to create and manage their own domains. A domain is a set of instances created using a common set of installed binaries in a single system.

Domain Administration Server (n.) The Domain Administration Server is a specially designated Application Server instance that handles all administrative tasks for the Application Server. It maintains and updates the central repository for Application Server configuration information. If the Domain Application Server isn't running, administrative tasks are unavailable.

domain administrator (n.) A user who has administrative privileges to create, modify, and delete mail users, mail lists, and family accounts in a hosted domain by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs. By default, this user can act as a message store administrator for all messaging servers in the topology.

domain alias (n.) A domain entry that points to another domain. By using aliases, hosted domains can have several domain names.

domain directory (n.) The directory for an Application Server domain, which contains at least one instance directory. This is what the server root is called in the Application Server.

domain hosting (n.) The process of hosting a domain. The ability to host one or more domains on a shared messaging server. For example, the domains `example.com` and `example.org` might both be hosted on the `example.com` mail server. Users send mail to and receive mail from the hosted domain. The name of the mail server does not appear in the email address.

domain name (1) (n.) A host name used in an email address.

(2) (n.) A unique name that defines an administrative organization. Domains can contain other domains. Domain names are interpreted from right to left. For example, `example.com` is both the domain name of the Example Company and a subdomain of the top-level `com` domain. The `example.com` domain can be further divided into subdomains such as `corp.example.com`, and so on. See also host name, fully qualified domain name.

domain name system See DNS.

domain organization (n.) A subdomain below a hosted domain in the organization tree. Domain organizations are useful for companies that wish to organize their user and group entries along departmental lines.

domain part (n.) The part of an email address to the right of the "at" sign (`@`). For example, `example.com` is the domain part of the email address `jdoe@example.com`.

domain quota (n.) The amount of space allocated to a domain for email messages. The amount of space is configured by the system administrator.

domain registry (n.) A single data structure that contains domain-specific information for all the domains created and configured on an installation of a server, such as domain name, domain location, domain port, domain host.

domain rewrite rules See rewrite rule.

domain template (n.) The part of a rewrite rule that defines how the host and domain portion of an address is rewritten. The template can include a full static host and domain address or a single field substitution string, or both.

double failure (n.) Simultaneous failure of one or more mirror node pairs in the HADB. See HADB, HADB node, active node, spare node, mirror node, and data redundancy unit

drop word See stop word.

DRU See data redundancy unit.

DSA (directory system agent) (n.) An X.500 term for a Directory Server.

DSCC See Directory Service Control Center.

DSE (directory server entry) (n.) An entry, or DSA-specific entry, that has additional server-specific information associated with it. A DSE such as the Root DSE or schema DSE has different attributes on each server.

DSP (digital signal processing) (n.) The conversion of signals from analog to digital. A DSP cvard is required to access Portal Server software using a phone for voice access.

DSML (directory services markup language) (n.) A family of document formats for representing XML markup language that enable you to represent directory services in XML. Java Enterprise System Directory Server 5.2 conforms to version 2 of the DSML standard (DSMLv2).

DSN (n.) See delivery status notification.

dsservd (n.) A daemon that accesses the database files that hold the directory information and communicates with directory clients using the LDAP protocol.

dssetup (n.) A Java Enterprise System Directory Server preparation tool that makes an existing Directory Server ready for use by a Java Enterprise System Messaging Server.

DTD (document type definition) (n.) An optional part of the XML document prolog, as specified by the XML standard. The DTD specifies constraints on the valid tags and tag sequences that can be in the document. The DTD has a number of shortcomings, however, and this has led to various schema proposals. For example, the DTD entry `<!ELEMENT username (#PCDATA)>` says that the XML element called `username` contains parsed character data-that is, text alone, with no other structural elements under it. The DTD includes both the local subset, defined in the current file, and the external subset, which consists of the definitions contained in external DTD files that are referenced in the local subset using a parameter entity.

durable subscription (n.) In the JMS publish and subscribe delivery model, a subscription that continues to exist whether or not there is a current active subscriber object. If there is no active subscriber, the JMS provider retains the subscription's message*s* until they are received by the subscription or until they expire.

DWP (database wire protocol) (n.) A Calendar Server proprietary protocol that allows multiple servers to be linked together within the same Calendar Server system to form a distributed calendar store. The Calendar Servers uses DWP to retrieve remote data stored in the calendar database.

dynamic deployment (n.) In the Application Server, deployment or redeployment of an J2EE application or module is dynamic; that is, no server restart is required. See also dynamic reloading.

dynamic group (n.) A mail group defined by an LDAP search URL. Users usually join the group by setting an LDAP attribute in their directory entry.

dynamic reloading (n.) The process of modifying and reloading a previously deployed component without going through the full deployment process and without restarting the server. By default, servlets, pages created with JavaServer Pages™ technology (JSP technology), and enterprise bean components can be dynamically reloaded. See also dynamic deployment.

dynamic web application (n.) Refers to servlets, JSP™ pages, content providers, or anything else that needs to be processed by the Java web container that is accessed by the user's browser. For Java Enterprise System Portal Server, the application gets installed in the web server.

E

EAR file (enterprise archive file) (n.) An archive file that contains a J2EE application. EAR files have the `.ear` extension.

ebXML (Electronic Business XML) (adj.) A group of specifications designed to enable enterprises to conduct business through the exchange of XML-based messages. It is sponsored by OASIS and the United Nations Centre for the Facilitation of Procedures and Practices in Administration, Commerce and Transport (U.N./CEFACT).

ebXML registry (Electronic Business XML registry) (n.) A federated registry and repository that manages all types of electronic content described by standard and extensible metadata.

ECC (elliptic curve cryptography) (n.) A public-key cryptography for mobile or wireless environments that operates on elliptic curves.

e-commerce (electronic commerce) (n.) A term for business conducted over the Internet.

EHLO command (n.) An SMTP command that queries a server to find out if the server supports extended SMTP commands. Defined in RFC 1869.

EIS (enterprise information system) (n.) The applications that constitute an enterprise's existing system for handling company-wide information. These applications provide an information infrastructure for an enterprise. An enterprise information system offers a well-defined set of services to its clients. These services are exposed to clients as local or remote interfaces or both. Examples of enterprise information systems include enterprise resource planning systems, mainframe transaction processing systems, and legacy database systems. Specific examples include R/3, PeopleSoft, Tuxedo, and CICS.

EIS resource (n.) A resource that provides enterprise information system-specific functionality to its clients. Examples are a record or set of records in a database system, a business object in an enterprise resource planning system, and a transaction program in a transaction processing system.

EJB container (n.) A container that implements the EJB component contract of the J2EE architecture. This contract specifies a runtime environment for an enterprise bean that includes security, concurrency, life-cycle management, transactions, deployment, naming, and other services. An EJB container is provided by an EJB or J2EE server. See also container.

EJB container provider (n.) A vendor that supplies an EJB container.

EJB context (n.) An object that allows an enterprise bean to invoke services provided by the container and to obtain the information about the caller of a client-invoked method.

EJB home object (n.) An object that provides the life-cycle operations (create, remove, find) for an enterprise bean. The class for the EJB home object is generated by the container's deployment tools. The EJB home object implements the enterprise bean's home interface. The client references an EJB home object to perform life-cycle operations on an EJB object. The client uses a JNDI name to locate an EJB home object.

EJB JAR file (n.) An archive file that contains an EJB module. EJB JAR files have the `.jar` extension.

EJB module (n.) A deployable unit that consists of one or more enterprise bean*s* and an EJB deployment descriptor. See also module.

EJB object (n.) An object whose class implements the enterprise bean*'s* remote interface. A client never references an enterprise bean instance directly; a client always references an EJB object. The class of an EJB object is generated by a container's deployment tools.

EJB server (n.) Software that provides services to an EJB container. For example, an EJB container typically relies on a transaction manager that is part of the EJB server to perform the two-phase commit across all the participating resource managers. The J2EE architecture assumes that an EJB container is hosted by an EJB server from the same vendor, so it does not specify the contract between these two entities. An EJB server can host one or more EJB containers.

EJB server provider (n.) A vendor that supplies an EJB server.

EJB™ QL (EJB Query Language) (n.) Defines the queries for the finder and select methods of an entity bean having container-managed persistence. A subset of SQL92, EJB QL has extensions that allow navigation over the relationships defined in an entity bean's abstract schema.

EJB technology (Enterprise JavaBeans™ technology) (n.) A component architecture for the development and deployment of object-oriented, distributed, enterprise-level applications. Applications written using the Enterprise JavaBeans architecture are scalable, transactional, and secure. See also enterprise bean.

ejbc utility (n.) The compiler for enterprise beans. This utility checks all EJB classes and interfaces for compliance with the EJB specification and generates stubs and skeletons.

element (n.) A member of a larger set, for example, a data unit within an array or a logic element. In an XML file, an element is the basic structural unit, delimited by tags. An XML element contains subelements or data and might contain attributes.

elliptic curve cryptography See ECC.

empty tag (n.) An XML tag that does not enclose any content.

encryption (n.) Process of protecting information from unauthorized use by making the information unintelligible. Some encryption methods employ codes, called keys, which are used to encrypt the information. See also decryption.

endpoint (1) (n.) The IP address or host name of a machine in a load-balanced cluster.

(2) (n.) In the Java Message Service, a message consumer. See message-driven bean.

(3) (n.) A Java class, typically a servlet or stateless session bean, annotated with the `javax.jws.WebService` annotation. This annotation defines the class as a web service endpoint, which receives messages from web service clients.

end user (n.) A person who uses a distributed application, often through a graphical user interface, such as an Internet browser or mobile device GUI. the number of concurrent end users supported by an application is an important determinant of the deployment architecture of the application.

ENS See event notification service.

enterprise bean (n.) A J2EE component that implements a business task or business entity and is hosted by an EJB container; either an entity bean, message-driven bean, or session bean. See also container.

enterprise bean provider (n.) An application developer who produces enterprise bean classes, remote and home interfaces, and deployment descriptor files, and packages them in an EJB JAR file.

enterprise network (n.) A network that consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and is used by the company's mission-critical applications.

entity (1) (n.) In XML files, a distinct, individual item that can be included in an XML document by referencing it. Such an entity reference can name an entity as small as a character (for example, `<`, which references the less-than symbol or left angle bracket, <). An entity reference can also reference an entire document, an external entity, or a collection of DTD definitions.

entity bean (n.) An EJB 1.x or 2.x enterprise bean that represents persistent data maintained in a database. An entity bean can manage its own persistence or can delegate this function to its container. An entity bean is identified by a primary key. If the container in which an entity bean is hosted

crashes, the entity bean, its primary key, and any remote references survive the crash. Entity beans are always transactional and multiuser aware. See also persistence, message-driven bean, read-only bean, and session bean.

entity reference (n.) A reference to an entity that is substituted for the reference when the XML document is parsed. It can reference a predefined entity such as `<` or reference one that is defined in the DTD. In the XML data, the reference could be to an entity that is defined in the local subset of the DTD or to an external XML file (an external entity). The DTD can also carve out a segment of DTD specifications and give it a name so that it can be reused (included) at multiple points in the DTD by defining a parameter entity.

entropy (n.) A measure of the randomness in a closed system. Specifically in the context of SSL, multiple seeds are used in order to introduce entropy (ensure randomness) in random number generation.

entry (n.) A group of attributes and a unique distinguished name.

entry distribution (n.) Method of distributing directory entries across more than one server in order to scale to support large numbers of entries.

entry ID list (n.) A list of entry IDs. Each index that the directory uses is composed of a table of index keys and matching entry ID lists. The entry ID list is used by the directory to build a list of candidate entries that might match the client application's search request.

enumeration (n.) The phase of a robot's operation in which the robot seeks resources, including extracting and following hypertext links.

envelope (n.) A container for transport information about the sender and the recipient of an email message. This information is not part of the message header. Envelopes are used by various email programs as messages are moved from place to place. Users see only the header and body of a message.

envelope field (n.) A named item of information, such as `RCPT TO`, in a message envelope.

equality index (n.) An index which allows you to search efficiently for entries containing a specific attribute value.

ERP (enterprise resource planning) (n.) A multi-module software system that typically includes a relationship database and applications for managing purchasing, inventory, personnel, customer service, shipping, financial planning, and other important aspects of the business.

error handler (n.) A program that handles errors. In Messaging Server, the error handler issues error messages and processes error-handler action forms after the postmaster fills them out.

error handler action form (n.) A form sent to the postmaster account that accompanies a received message that Messaging Server cannot handle. The postmaster fills out the form to instruct the server how to process the message.

ESMTP See extended simple mail transfer protocol.

ESP (n.) enterprise service provider.

ETRN command (n.) An SMTP command enabling a client to request that the server start the processing of its mail queues for messages that are waiting at the server for the client machine. Defined in RFC 1985.

event (1) (n.) An entry with an associated date and time in a calendar. For example, an event might be a new meeting or appointment on a calendar.

(2) (n.) A named action that triggers a response from a module or external Java Naming and Directory Interface ™ (JNDI) resource.

(3) (n.) A change in the state, mastery, severity, or description of a managed object.

(4) (n.) In the Application Server, an occurrence that triggers the action associated with a server self-management rule. See also management rule.

event notification service (n.) A generic service that accepts reports of server-level events that can be categorized and then notifies other servers that have registered interest in certain categories of events. Allows the Java Naming and Directory Interface™ (JNDI) Service to act as a bridge to a remote JNDI server.

expander (n.) Part of an electronic mail delivery system that allows a message to be delivered to a list of addressees. Mail expanders are used to implement mail lists. Users send messages to a single address (for example, `users@example.com`) and the mail expander takes care of delivery to the mailboxes in the list. Also called mail exploders. See also EXPN command.

expansion (n.) The act of converting a message addressed to a mail list into enough copies for each mail list member. Applies to the MTA processing of mail lists.

expires header (n.) The expiration time of the returned document specified by the remote server.

EXPN command (n.) An SMTP command for expanding a mail list. Defined in RFC 821.

expunge a message (v.) To permanently remove a message that has been deleted from the INBOX. See also delete a message, purge a message.

extended simple mail transfer protocol (n.) An Internet message transport protocol. ESMTP adds optional commands to the SMTP command set for enhanced functionality, including the ability for ESMTP servers to discover which commands are implemented by the remote site.

extensible markup language See XML.

extensible style language See XSL.

extensible style language transformation See XSLT.

external entity (n.) An entity that exists as an external XML file, which is included in the XML document using an entity reference.

external subset (n.) That part of a DTD that is defined by references to external DTD files.

extracting (n.) The process of locating hypertext links in a document. Each extracted link is added to the URL pool for further processing.

extranet (n.) An extension of a company's intranet onto the Internet to allow customers, suppliers, and remote workers access to the data.

F

facade (n.) Where an application-specific stateful session bean is used to manage various Enterprise JavaBeans™ components.

facility (n.) In a Messaging Server log-file entry, a designation of the software subsystem (such as Network or Account) that generated the log entry.

factory class (n.) A class that creates persistence managers. See also connection factory

failover (1) (n.) A recovery process where the state of a session, servlet, or stateful session bean can transparently survive a server crash. See also persistence, session failover.

(2) (n.) The automatic transfer of a computer service from one system to another to provide redundant backup.

family group administrator (n.) A user who has administrative privileges to add and remove family members in a family group. This user can grant family group administrative access to other members of the group.

fancy indexing (n.) A method of indexing that provides more information than simple indexing. Fancy indexing displays a list of contents by name with file size, last modification date, and an icon reflecting file type. Because of this, fancy indexes might take longer than simple indexes for the client to load.

fatal error (n.) A fatal error occurs in the SAX parser when a document is not well formed or otherwise cannot be processed. See also warning.

federated identity (n.) The amalgamation of the account information in all service providers that are accessed by one user (for example, personal data, authentication information, buying habits and history, shopping preferences, and so on). The information is administered by the user and, with the user's consent, securely shared with the user's providers of choice.

federation cookie (n.) A federation cookie is a cookie implemented by Access Manager with the name fedCookie. It can have a value of either yes or no based on the principal's federation status. It is not a defined part of the LAP specifications.

federation termination (n.) The process by which users cancel affiliations established between the user's identity provider and federated service provider accounts. Also called defederation.

file cache (n.) The file cache contains information about files and static file content. The file cache is turned on by default.

file extension (n.) The last part of a file name that typically defines the type of file. For example, in the file name `index.html`, the file extension is `html`.

file transfer protocol See FTP.

file type (n.) The format of a given file. For example, a graphics file does not have the same file type as a text file. File types are usually identified by their file extension. See also file extension.

filter (1) (n.) In a search request, a pattern which an entry in the scope of the search must match for that entry to be returned in the search response. Filters are also used in constructing role and access control definitions.

(2) (n.) A set of rules that define particular types of resources. These filters are used by site definitions to define types of resources the robot should accept or ignore.

(3) (n.) An object that can transform the header or content (or both) of a request or response. Filters differ from web components in that they usually do not themselves create responses but rather modify or adapt the requests for a resource, and modify or adapt responses from a resource. A filter should not have any dependencies on a web resource for which it is acting as a filter so that it can be composable with more than one type of web resource.

filter chain (n.) A concatenation of XSLT transformations in which the output of one transformation becomes the input of the next.

filtered role (n.) A method by which roles are assigned to entries. Allows you to assign entries to the role depending upon the attribute contained by each entry. You do this by specifying an LDAP filter. Entries that match the filter are said to possess the role.

filtering (n.) The process of determining whether a document is part of a site that should be included in the index.

finder method (n.) A method defined in the home interface that enables clients to look up an entity bean or a collection of beans in a globally available directory.

firewall (n.) A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. Firewalls are commonly used to protect information such as a network's email and data files within a physical building or organization site.

flexible log format (n.) A format used by the server for entering information into the access logs.

folder (n.) A named collection of messages. Folders can contain other folders. Also known as a mailbox. See also personal folder, public folder, shared folder, INBOX.

form action handler (n.) A specially defined method in servlet or application logic that performs an action based on a named button on a form.

form-based authentication (n.) An authentication mechanism in which a Web container provides an application-specific form for logging in. This form of authentication uses Base 64 encoding and can expose user names and passwords unless all connections are over SSL.

FORTEZZA (n.) An encryption system used by U.S. government agencies to manage sensitive but unclassified information.

forwarding See message forwarding.

foundation profile (n.) A set of APIs together with the CDC that provide a J2ME™ application runtime environment targeted at next generation applications, consumer electronic, and embedded devices.

fragmentation (n.) The MIME feature that allows the breaking of a large message into smaller messages. See also defragmentation.

fresh start (n.) Starting the robot from its starting points. A fresh start deletes the robot\qs state information, causing the robot to begin its next run from its initial state. Opposite of a restart.

FSMO role (Flexible Single-Master Operation role) (n.) The mechanism used by Active Directory to prevent update conflicts in multimaster replication deployments. Some objects are updated in a single-master mode even if the deployment is multimaster, which is very similar to the old concept of a Primary Domain Controller (PDC) in Windows NT domains. There are five FSMO roles in an Active Directory deployment, but only the PDC-emulator role affects Identity Synchronization for Windows. Because password updates are replicated immediately only to the Active Directory domain control with the PDC emulator role, Identity Synchronization for Windows use this domain controller for synchronization. Otherwise, synchronization with the Directory Server might be delayed for several minutes.

FTP (file transfer protocol) (n.) An Internet protocol that allows files to be transferred from one computer to another over a network.

fully qualified domain name (n.) The full name of a system, containing its host name and its domain name. For example: `example.sun.com`, where `example` is the host name (of a server) `sun.com` in the domain name.

G

gateway (n.) A system that translates from one native format to another. Examples include X.400 to and from RFC 822 electronic mail gateways. A machine that connects two or more electronic mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be complex. Generally requires a store-and-forward scheme whereby the message is received from one system completely before it is transmitted to the next system after suitable translations.

general access (n.) A level of user access. When granted, indicates that all authenticated users can access directory information.

general ACL (n.) A named access control list in the Java Enterprise System Directory Server that relates a user or group with one or more permissions. This list can be defined and accessed arbitrarily to record any set of permissions.

general entity (n.) An entity that is referenced as part of an XML document's content, as distinct from a parameter entity, which is referenced in the DTD. A general entity can be a parsed entity or an unparsed entity.

generation (n.) The phase of a robot's operation in which the robot produces a resource description for each resource discovered in the enumeration phase.

generic servlet (n.) A servlet that extends `javax.servlet.GenericServlet`. Generic servlets are protocol-independent: They contain no inherent support for HTTP or any other transport protocol. See also HTTP servlet.

GIF (graphics interchange format) (n.) A cross-platform image format originally created by CompuServe. GIF files are usually much smaller in size than other graphic file types, for example, TIFF. GIF is one of the most common interchange formats. GIF images are readily viewable on UNIX, Microsoft Windows, and Apple Macintosh systems.

global database connection (n.) A database connection available to multiple components. Requires a resource manager.

global transaction (n.) A transaction that is managed and coordinated by a transaction manager and can span multiple databases and processes. The transaction manager typically uses the XA protocol to interact with the database backends. See also local transaction.

GMT (Greenwich Mean Time) (n.) The mean solar time of the meridian of Greenwich, England, and the time standard against which all other time zones in the world are referred. GMT is not affected by Daylight Savings Time or Summer Time.

granularity level (n.) The approach to dividing an application into pieces. A *high level of granularity* means that the application is divided into many smaller, more narrowly defined Enterprise JavaBeans™ components. A *low level of granularity* means the application is divided into fewer pieces, producing a larger program.

greeting form (n.) A message usually sent to users when an account is created for them. This form acts as confirmation of the new account and verification of its contents.

group (1) (n.) An authenticated set of users classified by common traits such as job title or customer profile. Groups are also associated with a set of roles, and every user that is a member of a group inherits all the roles assigned to that group. The two types of groups are default user group and standard user group. Group membership is usually maintained by a local system administrator. See also user, role.

(2) (n.) Several LDAP mail entries that are organized under a distinguished name. Usually used as a mail list, but might also be used to grant certain administrative privileges to members of the group. See also dynamic group, static group.

group folders (n.) These folders that contain shared and group folders. See also public folder, shared folder.

group ID (n.) The group for Calendar Server files such as counters and logs. The group ID is stored in the `ics.conf` file in the `local.servergid` parameter. Also known as GID.

group scheduling engine (n.) The Calendar Server process that handles group scheduling. This engine enables a user to schedule events with other calendar users on the same server or on a different server. The other users can then modify, cancel, or reply to the event.

GUI (n.) graphical user interface.

H

HA See high availability.

HA data service See data service.

HADB See high availability database.

HADB node (n.) A set of HADB processes, a dedicated area of shared memory, and one or more secondary storage devices used for storing and updating session data. Each active (data storage) node must have a mirror node; therefore nodes occur in pairs. In addition, two or more spare nodes can be included to maximize availability. If an active node fails and cannot recover within a timeout period, the spare node copies the data from the mirror node and becomes active. See also high availability database

handle (n.) An object that identifies an enterprise bean. A client can serialize the handle and then later deserialize it to obtain a reference to the bean.

hard restart (n.) The termination of a process or service and its subsequent restart. See also soft restart.

hashdir (n.) A command-line utility for determining which directory contains the message store for a particular user.

HDML (Handheld Device Markup Language) (n.) Openwave's proprietary language to program mobile devices that use Openwave browsers.

header (n.) The portion of an email message that precedes the body of the message. The header is composed of field names followed by a colon and then values. Headers contain information useful to email programs and to users trying to make sense of the message. For example, headers include delivery information, summaries of contents, tracing, and MIME information. Headers tell whom the message is for, who sent it, when it was sent, and what it is about. Headers must be written according to RFC 822 so that email programs can read them.

header field (n.) A named item of information, such as “From:” or “To:”, in a message header. Also known as a header line.

heartbeat (n.) In the Application Server, a periodic message sent to all available servers in a cluster. Lack of a heartbeat after a specified interval and number of retries might trigger failover.

heuristic decision (n.) The transactional mode used by a particular transaction. A transaction has to either Commit or Rollback.

high availability (n.) Enables the detection of a service interruption and provides recovery mechanisms in the event of a system failure or process fault. In addition, high availability allows a backup system to take over the services in the event of a primary system failure. Also known as HA.

high availability database (HADB) (n.) A highly scalable, highly available session state persistence infrastructure. Application Server uses the HADB to store HTTP session states and stateful session bean states. See also HADB node, active node

home handle (n.) An object that can be used to obtain a reference to the home interface. A home handle can be serialized and written to stable storage and deserialized to obtain the reference.

home interface (n.) An interface that defines the methods that enable a client to create and remove an EJB 1.x or 2.x enterprise bean. The home interface of a session bean defines `create` and `remove` methods, whereas the home interface of an entity bean defines `create`, finder, and `remove` methods. See also remote interface.

home page (n.) A document that exists on the server and acts as a catalog or entry point for the server’s contents. The location of this document is defined within the server’s configuration files.

hop (n.) A transmission between two computers.

horizontal scalability (n.) The Calendar Server’s capability to run on a single server or as a group of processes that are spread across multiple servers with a wide variety of possible configuration options.

host (n.) The machine on which one or more servers reside.

hosted domain (n.) An email domain that is outsourced to an ISP. That is, the ISP provides email domain hosting for an organization by operating and maintaining the email services for that organization. A hosted domain shares the same Java Enterprise System Messaging Server host with other hosted domains. In earlier LDAP-based email systems, a domain was supported by one or more email server hosts. With Messaging Server, many domains can be hosted on a single server. For each hosted domain, there is an LDAP entry that points to the user and group container for the domain. Also known as a virtual hosted domain or a virtual domain

host-IP authentication (n.) A security mechanism used for limiting access to the Java Enterprise System Administration Server or the files and directories on a web site by making them available only to clients using specific computers.

host name (n.) The name of a particular machine within a domain. The host name is the IP host name, which might be either a "short-form" host name (for example, `mail`) or a fully qualified host name. The fully qualified host name consists of the host name and the domain name. For example, `mail.example.com` is the host name `mail` in the domain `example.com`. Host names must be unique within their domains. Your organization can have multiple machines named `mail`, as long as the machines reside in different subdomains, for example, `mail.corp.example.com` and `mail.field.example.com`. Host names always map to a specific IP address. See also fully qualified domain name, IP address.

host-name hiding (n.) The practice of using domain-based email addresses that do not contain the name of a particular internal host.

HTML (hypertext markup language) (n.) A markup language for hypertext documents on the Internet. HTML enables the embedding of images, sounds, video streams, form fields, references to other objects with URLs, and basic text formatting. Each block of text is surrounded by codes that indicate the nature of the text.

HTML page (n.) A page coded in HTML and intended for display in a web browser.

HTTP (hypertext transfer protocol) (n.) The Internet protocol based on Transmission Control Protocol/Internet Protocol that fetches hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client.

HTTPD (hyptertext transfer protocol daemon) (n.) An abbreviation for the HTTP daemon or service, which is a program that serves information using the HTTP protocol.

HTTP-NG (hypertext transfer protocol-next generation) (n.) The next generation of hypertext transfer protocol.

HTTPS (hypertext transfer protocol secure) (n.) A secure version of HTTP implemented using the secure socket layer protocol.

HTTP servlet (n.) A servlet that extends `javax.servlet.HttpServlet`. These servlets have built-in support for the HTTP protocol. See also generic servlet.

hub (n.) A host that acts as the single point of contact for the system. When two networks are separated by a firewall, for example, the firewall computer often acts as a mail hub.

hypertext transfer protocol secure See HTTPS.

I

iCalendar Message-Based Interoperability Protocol (n.) This protocol specifies a binding from the iCalendar Transport-Independent Interoperability Protocol to Internet email-based transports. This protocol is also known as iMIP. iMIP is defined in RFC 2447.

iCalendar Transport-Independent Interoperability Protocol (n.) An Internet protocol based on the iCalendar object specification that provides scheduling interoperability between different calendar systems. This protocol is also known as iTIP. iTIP is defined in RFC 2446.

IDE (integrated development environment) (n.) Software that allows you to create, assemble, deploy, and debug code from a single graphical user interface.

IDENT See Identification Protocol.

Identification Protocol (n.) A protocol that provides a means to determine the identity of a remote process responsible for the remote end of a particular TCP connection. This protocol is also known as IDENT. Defined in RFC 1413.

identity (n.) A set of information by which one end user is definitively distinguished. By defining a user identifier and password, an email address, personal preferences (such as style of music, or opt-in/opt-out marketing decisions) and other information specific to a particular business (a bank account number or ship-to address), end users distinguish themselves from others who also use the service.

identity federation (n.) A process that occurs when a user chooses to unite distinct service provider accounts with identity provider accounts. Users retain their individual account information with each provider while simultaneously establishing a link that allows the exchange of authentication information between provider accounts. Also called account federation.

identity provider (n.) A service provider that specializes in providing authentication services. As the administrating service for authentication, the identity provider maintains and manages identity

information. Authentication provided by an identity provider is honored by all service providers with whom the identity provider is affiliated.

identity service (n.) An identity service is a Web service that acts upon a resource to retrieve, update, or perform some action on data attributes related to a Principal (an identity). An example of an identity service might be a corporate phone book or calendar service.

IDL (interface definition language) (n.) A language used to define interfaces to remote CORBA objects. The interfaces are independent of operating systems and programming languages. Describes functional interfaces for remote procedure calls (RPC), so that a compiler can generate proxy and stub code that marshals parameters between machines.

idle state (n.) A type of state in which the robot is still running but has processed all the URLs in its URL pool. In this state, the robot can still respond to status requests.

iHTML (i-mode hypertext markup language) (n.) The language used with NTT DoCoMo's Japanese i-mode service.

IIOP (Internet Inter-ORB Protocol) (n.) A transport-level protocol used by both Remote Method Invocation (RMI) over IIOP and Common Object Request Broker Architecture (CORBA). Used for communication between CORBA object request brokers.

IIOP cluster (n.) An IIOP cluster that has been configured for high availability of RMI/IIOP requests.

IIOP endpoint (n.) An IIOP listener that has been configured for an IIOP cluster to enable high availability of RMI/IIOP requests.

IIOP listener (n.) A listen socket that listens on a specified port and accepts incoming connections from CORBA-based client applications.

imagemap (1) (n.) A process that makes areas of an image active, letting users navigate and obtain information by clicking the different regions of the image with a mouse.

(2) (n.) A CGI program that is used to handle imagemap functionality in other HTTPD implementations.

IMAP4 (Internet Message Access Protocol Version 4) (n.) A standard protocol that allows users to be disconnected from the main messaging system and still be able to process their mail. The IMAP specification allows for administrative control for these disconnected users and for the synchronization of the users' message store once they reconnect to the messaging system.

iMIP See iCalendar Transport-Independent Interoperability Protocol.

immediate subordinate (n.) In the DIT, an entry is an immediate subordinate of another entry if its distinguished name is formed by appending its relative distinguished name to the distinguished name of the parent entry.

immediate superior (n.) In the DIT, an entry is the immediate superior of another entry if its distinguished name, followed by the relative distinguished name of the other entry, forms the distinguished name of the child entry.

impersonation (n.) An act whereby one object assumes the identity and privileges of another object without restrictions and without any indication visible to the recipients of the impersonator's calls that delegation has taken place. Impersonation is a case of simple delegation.

import agent (n.) The process used during importing.

importing (n.) The process of bringing new or updated resource descriptions from another database into the Search Engine.

imsadmin commands (n.) A set of command-line utilities for managing domain administrators, users, and groups.

imsimta commands (n.) A set of command-line utilities for performing various maintenance, testing, and management tasks for the MTA.

inactive boot environment (n.) An environment which is not currently booted or designated for activation upon the next reboot. See also active boot environment.

INBOX (n.) The name reserved for a user's default mailbox. Used for mail delivery. INBOX is the only folder name that is case-insensitive, which means that INBOX, Inbox, and inbox are all valid names for a user's default mailbox.

index (n.) A centralized, searchable database of resources or documents. Also known as a catalog.

indexing (n.) The process of providing a centralized, searchable database of resources. Also known as cataloging.

index key (n.) Each index that the directory uses is composed of a table of index keys and matching entry ID lists.

indirect CoS (n.) Identifies the template entry using the value of one of the target entry\qs attributes.

initialization parameter (n.) A parameter that initializes the context associated with a servlet.

inittab file (n.) (UNIX only) A file listing programs that need to be restarted if they stop for any reason. The file ensures that a program runs continuously. Because of its location, the file is also called `/etc/inittab`. This file is not available on all UNIX systems.

installation directory

(n.) The directory into which the binary (executable) files of a server are installed. For the Messaging Server, the installation directory is a subdirectory of the server root: *server-root*`/bin/msg/`. See also instance directory.

installation path

(n.) The full path under which Directory Server Enterprise Edition software is installed. You can choose the installation path when installing software for the first time.

instance directory

(n.) The directory that contains the files that define a specific instance of a server. For the Messaging Server, the instance directory is a subdirectory of the server root: *server-root*`/msg-`*instance*`/`, where *instance* is the name of the server as specified at installation. For the Application Server, the instance directory is a subdirectory of the domain directory. See also installation directory, server instance.

instance path

(n.) The full path under which data for a Directory Server or Directory Proxy Server server instance is located. You choose the instance path when creating a server instance.

Instant Messaging Client

(n.) The client that enables users to send and receive instant messages and alerts.

Instant Messaging multiplexor

(n.) A manager of client connections. Improves Instant Messaging Server scalability by allowing a large number of concurrent client connections to require only a few connections to the back-end Instant Messaging server. Instant Messaging clients connect to the multiplexor rather than to the Instant Messaging server itself. When installed on the public side of a firewall, the multiplexor protects the user database from intruders, leaving the Instant Messaging Server behind the firewall.

Instant Messaging Server

(1) (n.) Refers to the Java Enterprise System Messaging Server product itself, including all components (server, multiplexor, and Java Enterprise System Instant Messaging Server).

(2) (n.) The back-end server process within the product that handles incoming commands from Instant Messaging (through the Instant Messaging Server multiplexor). The Instant Messaging Server also communicates with the LDAP server in the authentication of Instant Messaging users. See also Instant Messaging multiplexor

intelligent agent

(n.) An object within a server that performs various requests (such as HTTP, NNTP, SMTP, and FTP requests) on behalf of the user. In a sense, the intelligent agent acts as a client to the server, making requests that the server fulfills.

international index

(n.) A type of search index. Speeds up searches for information in a DIT in which the attributes have language tags.

Internet Message Access Protocol Version 4

See IMAP4.

Internet Protocol

See IP.

intranet (n.) A network of Transmission Control Protocol/Internet Protocol networks within a company or organization. Intranets enable companies to employ the same types of servers and client software used for the World Wide Web for internal applications distributed over the corporate LAN. Sensitive information on an intranet that communicates with the Internet is usually protected by a firewall. See also firewall, extranet.

invalid user (n.) An error condition that occurs during message handling. When this error condition occurs, the message store sends a communication to the MTA and then deletes its copy of the message. The MTA bounces the message back to the sender and deletes its copy of the message.

IP (Internet Protocol) (n.) Protocol within the Transmission Control Protocol/Internet Protocol suite used to link networks worldwide. Developed by the United States Department of Defense and used on the Internet. The prominent feature of this suite is the IP protocol.

IP address (n.) A set of numbers separated by dots, such as `192.168.255.255`, that specifies the actual location of a machine on an intranet or the Internet. A 32-bit address assigned to hosts using Transmission Control Protocol/Internet Protocol.

ISDN (n.) Integrated Services Digital Network.

ISINDEX (n.) An HTML tag that turns on searching in the client. Documents can use a network navigator's capabilities to accept a search string and send it to the server to access a searchable index without using forms. In order to use the `ISINDEX` HTML tag, you must create a query handler.

ISMAP (n.) An extension to the `IMG SRC` tag used in an HTML document to tell the server that the named image is an imagemap.

ISO 3166 (n.) The international standard for country codes maintained by the International Organization for Standardization (ISO).

ISO 8601 (n.) An International Organization for Standardization standard that specifies the numeric representation of date and time. The Calendar Server uses ISO 8601 standard notations to represent date, time, and duration strings.

isolation level See transaction isolation level.

issued certificate (n.) A certificate that is issued by a certificate authority. See also self-generated certificate.

ISV (n.) Independent software vendor.

iTIP See iCalendar Transport-Independent Interoperability Protocol.

J

J2EE™ application (n.) Any deployable unit of J2EE platform functionality. This can be a single J2EE module or a group of modules packaged into an EAR file along with a J2EE application deployment descriptor. J2EE applications are typically engineered to be distributed across multiple computing tiers.

J2EE component (n.) A self-contained functional software unit supported by a container and configurable at deployment time. A web application, session bean, entity bean, message-driven bean, application client, or connector. These J2EE components are written in the Java™ programming language and are compiled in the same way as any program in the language. See also component.

J2EE module (n.) A software unit that consists of one or more J2EE components of the same container type and one deployment descriptor of that type. Modules can be deployed as stand-alone units or can be assembled into a J2EE application. See also life-cycle module, module.

J2EE platform (Java 2 Platform, Enterprise Edition) (n.) An environment for developing and deploying multi-tiered, web-based enterprise applications. The J2EE platform consists of a set of services, APIs, and protocols that provide the functionality for developing these applications.

J2EE product (n.) An implementation that conforms to the J2EE platform specification.

J2EE product provider (n.) A vendor that supplies a J2EE product.

J2EE server (n.) The runtime portion of a J2EE product. A J2EE server provides EJB or web containers or both. See also container.

J2ME™ platform (Java 2 Platform, Micro Edition) (n.) A highly optimized Java runtime environment targeting a wide range of consumer products, including pagers, cellular phones, screen phones, digital set-top boxes, and car navigation systems.

J2SE™ platform (Java 2 Platform, Standard Edition) (n.) The core Java technology platform.

JAF (JavaBeans™ Activation Framework) (n.) Integrates support for MIME data types into the Java platform. See also MIME data type.

JAR file contract (n.) A Java Archive file contract that specifies what information must be in the enterprise bean package.

JATO (n.) A library for converting between code written in the Java programming language and XML. Also known as Sun Java System Web Application Framework, or Application Framework. JATO is geared toward enterprise web application development. JATO combines concepts such as display fields, application events, component hierarchies, and a page-centric development approach.

Java 2 Platform, Enterprise Edition See J2EE platform.

Java 2 Platform, Micro Edition See J2ME platform.

Java 2 Platform, Standard Edition See J2SE platform.

JavaBean™ namespace (n.) A standard that allows you to specify a unique label to the set of element names defined by a package. A document using that package can be included in any other document without having a conflict between element names. The elements defined in the package are uniquely identified so that, for example, the parser can determine when an element should be interpreted according to your package and not according to that of another package.

JavaBeans Activation Framework See JAF.

JavaBeans component (n.) A Java class that can be manipulated by tools and composed into applications. A JavaBeans component must adhere to certain property and event interface conventions.

JavaBeans component architecture (n.) A portable, platform-independent reusable component model.

Java Enterprise System (n.) An integration of individual Sun software products into a software system that supports distributed enterprise applications.

Java ES See Java Enterprise System.

Java ES shared component See shared component.

JavaMail™ (API, extension) (n.) An API for sending and receiving email. Application code uses the Java Naming and Directory Interface™ (JNDI) service to locate JavaMail session resource objects using a JNDI name.

JavaScript™ programming language (n.) A compact, object-based scripting language for developing client and server Internet applications.

JavaServer Faces™™ conversion model (n.) A mechanism for converting between string-based markup generated by JavaServer Faces UI components and server-side Java objects.

JavaServer Faces event and listener model (n.) A mechanism for determining how events emitted by JavaServer Faces UI components are handled. This model is based on the JavaBeans component event and listener model.

JavaServer Faces expression language (n.) A simple expression language used by a JavaServer Faces UI component tag attributes to bind the associated component to a bean property or to bind the associated component's value to a method or an external data source, such as a bean property. Unlike JSP expression language expressions, JavaServer Faces EL expressions are evaluated by the JavaServer Faces implementation rather than by the web container.

JavaServer Faces navigation model (n.) A mechanism for defining the sequence in which pages in a JavaServer Faces application are displayed.

JavaServer Faces UI component (n.) A user interface control that outputs data to a client or allows a user to input data to a JavaServer Faces application.

JavaServer Faces UI component class (n.) A JavaServer Faces class that defines the behavior and properties of a JavaServer Faces UI component.

JavaServer Faces technology (n.) A framework for building server-side user interfaces for web applications written in the Java programming language.

JavaServer Faces validation model (n.) A mechanism for validating the data a user inputs to a JavaServer Faces UI component.

JavaServer Pages™™ technology See JSP technology.

Java Web Start software (n.) A web application launcher. With Java Web Start software, applications are launched by clicking on the web link. If the application is not present on the computer, Java Web Start automatically downloads the application and caches it on the computer. Once an application is downloaded to its cache, it can be launched from a desktop icon or from a browser link. No matter which method is used to launch the application, the most current version of the application is always presented.

JAXM (Java API for XML Messaging) (n.) A Java API that uses the SOAP standard to enable applications to send and receive document-oriented XML messages. These messages can be with or without attachments.

JAXP (Java API for XML Processing) (n.) An API for processing XML documents. JAXP leverages the parser standards SAX and DOM so that you can choose to parse your data as a stream of events or to build a tree-structured representation of it. JAXP supports the XSLT standard, giving you control over the presentation of the data and enabling you to convert the data to other XML documents or to other formats, such as HTML. JAXP provides namespace support, allowing you to work with schema that might otherwise have naming conflicts.

JAXR (Java API for XML Registries) (n.) A uniform and standard Java API for accessing different kinds of XML registries. Enables users to build, deploy, and discover web services. See also registry.

JAXR client (n.) A client program that uses the JAXR API to access a business registry through a JAXR provider.

JAXR provider (n.) An implementation of the JAXR API that provides access to a specific registry provider or to a class of registry providers that are based on a common specification.

JAX-RPC (Java API for XML-based RPC) (n.) A Java API that enables developers to build interoperable web applications and web services based on XML-based RPC protocols.

JDBC™ connection pool (n.) A pool that combines the JDBC data source properties used to specify a connection to a database with the connection pool properties.

JDBC resource (n.) A resource used to connect an application running within the application server to a database by way of an existing JDBC connection pool. Consists of a Java Naming and Directory Interface™ (JNDI) name (which is used by the application) and the name of an existing JDBC connection pool.

JDBC technology (Java DataBase Connectivity software) (n.) A standards-based set of classes and interfaces that enable developers to create data-aware components. The JDBC API implements methods for connecting to and interacting with data sources in a platform-independent and vendor-independent way. JDBC technology provides a call-level API for SQL-based database access.

JHTML (J-Sky hypertext markup language) Vodafone's proprietary language used to program Japanese J-Sky devices.

JMS (Java Message Service) (n.) A standard set of interfaces and semantics that define how a Java client accesses the facilities of a message service. These interfaces provide a standard way for programs written in the Java programming language to create, send, receive, and read messages.

JMSadministered object (Java Message Service administered object) (n.) A pre-configured Java Message Service object (JMS connection factory or JMS destination) created by an administrator for use by one or more JMS clients. The use of administered objects allows JMS clients to be isolated from the

proprietary aspects of a provider, thereby making the clients provider-independent. These objects are placed in a Java Naming and Directory Interface™ (JNDI) name space by an administrator and are accessed by JMS clients using JNDI lookups.

JMS API (Java Message Service API) (n.) A standard set of interfaces and semantics that define how a JMS client accesses the facilities of a JMS message service. These interfaces provide a standard way for programs written in the Java programming language to create, send, receive, and read messages.

JMS application (Java Message Service application) (n.) One or more JMS clients that exchange messages.

JMS client (Java Message Service client) (n.) An application or software component that interacts with other JMS clients using a JMS message service to exchange messages.

JMS connection factory (Java Message Service connection factory) (n.) The object administered by the Java Message Service that a JMS client uses to create a connection to a JMS message service.

JMS destination (Java Message Service destination) (n.) The physical destination in a JMS message service to which produced messages are delivered for routing and for subsequent delivery to consumers. This physical destination is identified and encapsulated by an JMS-administered object that a JMS client uses to specify the destination of incoming and outgoing messages.

JMS messages (Java Message Service messages) (n.) Asynchronous requests, reports, or events that are consumed by Java Message Service clients. A message has a header (to which additional fields can be added) and a body. The message header specifies standard fields and optional properties. The message body contains the data that is being transmitted.

JMS provider (Java Message Service provider) (n.) A product that implements the JMS interfaces for a messaging system and adds the administrative and control functions needed for a complete product.

JMS service (Java Message Service service) (n.) Software that provides delivery services for a Java Message Service messaging system, including connections to JMS clients, message routing and delivery, persistence, security, and logging. The message service maintains physical destinations to which JMS clients send messages and from which the messages are delivered to consuming clients.

JMS session (Java Message Service session) (n.) A single-threaded context for sending and receiving JMS messages. A JMS session can be non-transactional, locally transacted, or participating in a distributed transaction.

JNDI extension (Java Naming and Directory Interface extension) (n.) A standard extension to the Java platform that provides Java technology-enabled applications with a unified interface to multiple naming and directory services in the enterprise. As part of the Java Enterprise API set, JNDI enables connectivity to heterogeneous enterprise naming and directory services.

JNDI name (Java Naming and Directory Interface name) (n.) A name used to access a resource that has been registered in the JNDI naming service.

job controller (n.) The MTA component responsible for scheduling and executing tasks upon request by various other MTA components.

join rule (n.) A rule which specifies how entries in a Directory Proxy Server secondary data view are linked to entries in a primary data view, or how entries in one SQL table are linked to entries in another SQL table.

jspc utility (n.) The compiler for pages created with JSP technology. The utility checks all JSP pages for compliance with the JSP specification.

JSP™ action (n.) A JSP element that can act on implicit objects and other server-side objects or can define new scripting variables. Actions follow the XML syntax for elements, with a start tag, a body, and an end tag; if the body is empty it can also use the empty tag syntax. The tag must use a prefix. There are standard and custom actions.

JSP container (n.) A container that provides the same services as a servlet container and an engine that interprets and processes JSP pages into a servlet.

JSP container, distributed (n.) A JSP container that can run a Web application that is tagged as distributable and is spread across multiple Java virtual machines that might be running on different hosts.

JSP custom action (n.) A user-defined action described in a portable manner by a tag library descriptor and imported into a JSP page by a `taglib` directive. Custom actions are used to encapsulate recurring tasks in writing JSP pages.

JSP custom tag (n.) A tag that references a JSP custom action.

JSP declaration (n.) A JSP scripting element that declares methods, variables, or both in a JSP page.

JSP directive (n.) A JSP element that gives an instruction to the JSP container and is interpreted at translation time.

JSP document (n.) A JSP page written in XML syntax and subject to the constraints of XML documents.

JSP element (n.) A portion of a JSP page that is recognized by a JSP translator. An element can be a directive, an action, or a scripting element.

JSP expression (n.) A scripting element that contains a valid scripting language expression that is evaluated, converted to a `String`, and placed into the implicit `out` object.

JSP expression language (n.) A language used to write expressions that access the properties of JavaBeans components. EL expressions can be used in static text and in any standard or custom tag attribute that can accept an expression.

JSP page (n.) A text-based document containing static text and JSP elements that describes how to process a request to create a response. A JSP page is translated into and handles requests as a servlet.

JSP scripting element (n.) A JSP declaration, scriptlet, or expression whose syntax is defined by the JSP specification and whose content is written according to the scripting language used in the JSP page. The JSP specification describes the syntax and semantics for the case where the language page attribute is `"java"`.

JSP scriplet (n.) A JSP scripting element containing any code fragment that is valid in the scripting language used in the JSP page. The JSP specification describes what is a valid scriptlet for the case where the language page attribute is `"java"`.

JSP standard action (n.) An action that is defined in the JSP specification and is always available to a JSP page.

JSP tag file (n.) A source file containing a reusable fragment of JSP code that is translated into a tag handler when a JSP page is translated into a servlet.

JSP tag handler (n.) A Java programming language object that implements the behavior of a custom tag.

JSP tag library (n.) A collection of custom tags described using a tag library descriptor and Java classes. See also JSTL.

JSP™ technology (1) (n.) An extensible web technology that uses static data, JSP elements, and server-side Java objects to generate dynamic content for a client. Typically the static data is HTML or XML elements, and in many cases the client is a Web browser. Pages created with JSP technology combine the layout capabilities of a standard browser page with the power of a programming language.

(2) (n.) Extensions that enable all JSP technology metafunctions, including instantiation, initialization, destruction, access from other components, and configuration management. Reusable Java applications that run on a web server rather than in a web browser.

JSS See Network Security Services for Java (JSS).

JSSE (Java Secure Socket Extension) (n.) A set of packages that enable secure Internet communications.

JSTL (JavaServer Pages Standard Tag Library) (n.) A tag library that encapsulates core functionality common to many JSP applications. JSTL has support for common, structural tasks such as

iteration and conditionals, tags for manipulating XML documents, internationalization and locale-specific formatting tags, SQL tags, and functions.

JTA (Java transaction API) (n.) An API that allows applications and J2EE servers to access transactions.

JTS (Java transaction service) (n.) Specifies the implementation of a transaction manager that supports JTA and implements the Java mapping of the Object Management Group Object Transaction Service 1.1 specification at the level below the API.

K

key database (n.) A file that contains the key pair or pairs for a server's certificate or certificates. Also called a key file.

key-pair file See trust database.

keystore (n.) A file containing the keys and certificates used for authentication.

knowledge information (n.) Part of the directory service infrastructure information. The directory server uses knowledge information to pass requests for information to other servers.

knowledge reference (n.) Pointers to directory information stored in different databases.

L

last-modified header (n.) The last modification time of the document file that is returned in the HTTP response from the server.

LDAP (Lightweight Directory Access Protocol) (n.) Directory service protocol designed to run over TCP/IP and across multiple platforms. A simplification of the X.500 Directory Access Protocol (DAP) that allows a single point of management for storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data across Sun Java System servers. Directory Server uses the LDAP protocol.

LDAP database (n.) A database where lists of users and groups is stored for use in authentication.

LDAP data interchange format See LDIF.

LDAP filter (n.) A method of specifying a set of entries that is based on the presence of a particular attribute or attribute value.

LDAP referrals (n.) An LDAP entry that consists of a symbolic link (referral) to another LDAP entry. An LDAP referral consists of an LDAP host and a distinguished name. LDAP referrals are often used to reference existing LDAP data so that this data does not have to be replicated. The LDAP referrals are also used to maintain compatibility for programs that depend on a particular entry that might have been moved.

LDAP search string (n.) A string with replaceable parameters that defines the attributes used for directory searches. For example, an LDAP search string of "uid=%s" means that searches are based on the user ID attribute.

LDAP server (n.) A software server that maintains an LDAP directory and services queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP Server.

LDAP server failover (n.) A backup feature for LDAP servers. If one LDAP server fails, the system can switch over to another LDAP server.

LDAP URL (n.) A URL that provides the means of locating directory servers using DNS and then completing the query through LDAP. A sample LDAP URL is `ldap://ldap.example.com`.

LDAPv3 (n.) Version 3 of the LDAPv3 protocol.

LDBM (n.) LDAP database manager.

LDBM database (n.) A high-performance, disk-based database consisting of a set of large files that contain all of the data in Directory Server.

LDIF (LDAP Data Interchange Format) (n.) The format used to represent Directory Server entries in text form using *type*:*value* pairs.

leaf entry (n.) An entry under which there are no other entries. A leaf entry cannot be a branch point in a directory tree.

Legato NetWorker®® software (n.) A third-party backup utility distributed by Legato Systems, Inc.

level (n.) A designation of logging verbosity, meaning the relative number of types of events that are recorded in log files. For example, at a level of Emergency or SEVERE, very few events are logged. At a level of Informational or INFO, many events are logged.

Liberty-enabled client (n.) A Liberty-enabled client is a client that has, or knows how to obtain, information about the identity provider that a principal will use to authenticate to a service provider.

Liberty-enabled proxy (n.) A Liberty-enabled proxy is an HTTP proxy that emulates a Liberty-enabled client.

life cycle (1) (n.) The framework events of a J2EE component's existence. Each type of component has defining events that mark its transition into states in which it has varying availability for use. For example, a servlet is created and has its `init` method called by its container before invocation of its `service` method by clients or other servlets that require its functionality. After the call of its `init` method, it has the data and readiness for its intended use. The servlet's `destroy` method is called by its container before the ending of its existence so that processing associated with winding up can be done and resources can be released. The `init` and `destroy` methods in this example are callback method*s*. Similar considerations apply to the life cycle of all J2EE component types: enterprise beans, web components (servlets or JSP pages), applets, and application clients.

(2) (n.) A set of phases during which a request for a JavaServer Faces page is received, a UI component tree representing the page is processed, and a response is produced.

(3) (n.) The framework events of a server's runtime, from startup to shutdown, inclusive.

life-cycle event (n.) A stage in the server life cycle such as startup or shutdown.

life-cycle module (n.) A module that listens for and performs its tasks in response to events in the server life cycle.

Lightweight Directory Access Protocol See LDAP.

listener (n.) A class, registered with a posting object, that says what to do when an event occurs.

listen port (n.) The port that a server uses to communicate with clients and other servers.

listen socket (n.) The combination of port number and IP address. Connections between the server and clients happen on a listen socket.

LMTP (Local Mail Transfer Protocol) (n.) Similar to SMTP but does not require management of a mail delivery queue. In addition, LMTP provides a status code for each recipient of a message where SMTP provides only one status code for the message. Defined in RFC 2033.

load balancer (n.) Software that controls connections to multiple gateway machines to allow approximately equivalent loads on each of the available systems.

load balancing (n.) The process of distributing the application load across nodes in the cluster so that the client requests are serviced in a timely manner. Applies only to scalable services.

local database connection (n.) The transaction context in a local connection is local to the current process and to the current data source, not distributed across processes or across data sources.

locale (n.) A setting that identifies the collation order, character type, monetary format, and date and time format used to present data for users of a specific region, culture, or custom. The locale includes information on how data of a given language is interpreted, stored, or collated. The locale also indicates which code page should be used to represent a given language.

local interface (n.) An interface that provides a mechanism for a client that is located in the same Java™ Virtual Machine (JVM™ machine) with a session or entity bean to access that bean.

Local Mail Transfer Protocol See LMTP.

local part (n.) The part of an email address that identifies the recipient. See also domain part.

local session (n.) A user session that is only visible to one server.

local subset (n.) That part of the DTD that is defined within the current XML file.

local transaction (n.) A transaction that is native to one database and is restricted within a single process. Local transactions work only against a single backend. Local transactions are typically demarcated using a JDBC™ API. See also global transaction

log directory (n.) The directory in which all of a service's log files are kept.

log expiration (n.) The deletion of a log file from the log directory after it has reached its maximum permitted age.

logical architecture (n.) A design that depicts the logical building blocks of a distributed application and the relationships (or interfaces) between these building blocks. The logical architecture includes both the distributed application component*s* and the infrastructure services components needed to support them.

logical host (n.) A Messaging Server 2.0 (minimum) concept that includes an application, the disksets or disk groups on which the application data resides, and the network addresses used to access the cluster. This concept no longer exists in the SunPlex™ system.

log rotation (n.) The creation of a new log file to be the current log file. All subsequent logged events are written to the new current file. The log file that was the previous log file is no longer written to, but remains in the log directory.

lookup (n.) Same as a search, using the specified parameters for sorting data.

M

mailbox (n.) A place where messages are stored and viewed. See also folder.

mail client (n.) The programs that help users send and receive email. The mail client is the part of the various networks and mail programs with which users have the most contact. Mail clients create and submit messages for delivery, check for new incoming mail, and accept and organize incoming mail.

mail exchange record See MX record.

mailing list See mail list.

mailing list owner See mail list owner.

mail list (n.) A list of email addresses to which a message can be sent by way of a mail list address. Sometimes called a group.

mail list owner (n.) A user who has administrative privileges to add members to and delete members from the mail list.

mail relay (n.) A mail server that accepts mail from a user account or an MTA and relays it to the mail recipient's message store or another router.

mail router See mail relay.

managed bean creation facility (n.) A mechanism for defining the characteristics of a JavaBeans component used in a JavaServer Faces technology application.

managed object (n.) An SNMP data element that forms part of an MIB. In Directory Server, the managed objects are held in `cn=monitor`, and the SNMP agent provides the objects to the network management station. As with LDAP attributes, each managed object has a name and object identifier expressed in dot notation.

managed role (n.) Allows you to create an explicit enumerated list of members.

management information base See MTA.

management rule (n.) Associates a custom self-tuning, self-configuring, or self-healing action with a triggering event in the Application Server. See also event.

mapping (1) (n.) The ability to tie an object-oriented model to a relational model of data, usually the schema of a relational database. The process of converting a schema to a different structure.

(2) (n.) The mapping use users to security roles.

mapping tree (n.) A data structure that associates the names of suffixes (subtrees) with databases.

master agent See SNMP master agent.

master channel program (n.) A channel program that typically initiates a transfer to a remote system. See also slave channel program.

master directory server (n.) A read-write directory server that contains the data that will be replicated.

matching category (n.) A category that matches a search query which is returned as a result of a search submission.

matching document (n.) A document that matches a search query, which is returned as the result of a search submission.

matching rule (n.) A guideline for how the server compares strings during a search operation. In an international search, the matching rule tells the server what collation order and operator to use.

MD5 (n.) A message digest algorithm by RSA Data Security. MD5 can be used to produce a short digest of data that is unique with high probability.

MD5 signature (n.) A message digest produced by the MD5 algorithm.

MDB (message-driven bean) (n.) An enterprise bean that is an asynchronous message consumer. A message-driven bean has no state for a specific client, but its instance variables might contain state across the handling of client messages, including an open database connection and an object reference to an object based on the EJB™ architecture. A client accesses a message-driven bean by sending messages to the destination for which the message-driven bean is a message listener.

member (n.) A user or group who receives a copy of an email addressed to a mail list. See also mail list, expansion, moderator.

message (1) (n.) The fundamental unit of email that consists of a header and a body and is often contained in an envelope while it is in transit from the sender to the recipient.

(2) (n.) In the Java Message Service, an asynchronous request, report, or event consumed by a JMS client. A message has a header (to which additional fields can be added) and a body. The message header specifies standard fields and optional properties. The message body contains the data that is being transmitted. A message contains vital information needed to coordinate enterprise applications, in the form of precisely formatted data that describes specific business actions.

message access services (n.) The protocol servers, software drivers, and libraries that support client access to the Messaging Server message store.

message consumer (n.) An object created by a JMS session that is used for receiving messages sent to a destination.

message delivery (n.) The act that occurs when an MTA delivers a message to a local recipient (a mail folder or a program).

message-driven bean See MDB.

message forwarding (n.) The act that occurs when an MTA sends a message delivered to a particular account to one or more new destinations as specified by the account's attributes. Forwarding might be configurable by the user. See also message delivery, message routing.

message handling system See MHS.

message producer (n.) An object created by a JMS session that is used for sending messages to a destination.

Message Queue (n.) The messaging system that implements the Java™ Message Service (JMS) open standard. Sun Java System Message Queue is a JMS provider.

message queue (n.) The directory where messages accepted from clients and other mail servers are queued for immediate or deferred delivery.

Message Queue client runtime (n.) Software that provides JMS clients with an interface to the Java Enterprise System message server. The client runtime supports all operations needed for clients to send messages to destinations and to receive messages from such destinations.

Message Queue message server (n.) Software that provides delivery services for a Message Queue messaging system, including connections to JMS clients, message routing and delivery, persistence, security, and logging. The message server maintains physical destinations to which JMS clients send messages, and from which the messages are delivered to consuming clients.

message quota (n.) A limit defining how much disk space a particular folder can consume.

message routing (n.) The act of transferring a message from one MTA to another when the first MTA determines that the recipient is not a local account, but might exist elsewhere. Routing is normally configurable only by a network administrator. See also message forwarding.

message selector (n.) A way for a consumer to select messages based on property values (selectors) in JMS message headers. A message service performs message filtering and routing based on criteria placed in message selectors.

message service See Message Queue message server.

message store (n.) The database of all locally delivered messages for a Messaging Server instance. Messages can be stored on a single physical disk or stored across multiple physical disks.

message store administrator (n.) A user who has administrative privileges to manage the message store for a Messaging Server installation. This user can view and monitor mailboxes and specify access control to the store. Using proxy authorization rights, this user can run certain utilities for managing the store.

message store partition (n.) A message store or subset of a message store residing on a single physical file system partition.

message submission (n.) The client userAgent transfers a message to the mail server and requests delivery.

message transfer agent See MTA.

messaging (n.) A system of asynchronous requests, reports, or events used by enterprise applications that allows loosely coupled applications to transfer information reliably and securely.

Messaging Multiplexor See MMP.

Messaging Server administrator (n.) The administrator whose privileges include installation and administration of a Messaging Server instance.

messaging server base directory (n.) The directory into which all servers associated with a given Administration Server on a given host are installed. Typically designated *msg_svr_base*. See also installation directory.

Messenger Express (n.) A mail client that enables users to access their mailboxes through a browser-based (HTTP) interface. Messages, folders, and other mailbox information are displayed in HTML in a browser window. See also webmail.

Messenger Express Multiplexor (n.) A proxy messaging server that acts as a Multiplexor. The server allows you to connect to the HTTP service of Messaging Server (Messenger Express). The Messenger Express Multiplexor facilitates distributing mail users across multiple server machines.

metadata (n.) Information about a component, such as the component's name and specifications for component behavior. See also deployment descriptor.

metadevice state database replica (n.) A database, stored on disk, that records configuration and the state of all metadevices and error conditions. This information is important to the correct operation of Solstice DiskSuite™ software disksets.

metainformation (n.) Information about a resource, such as the name of the author, the title of a document, the date of creation, and so on. The Search Engine robot uses metainformation as well as document contents when creating resource descriptions.

method-binding expression (n.) An expression in the JavaServer Faces expression language that refers to a method of a backing bean. This method performs either event handling, validation, or navigation processing for the UI component whose tag uses the method-binding expression.

method permission (n.) An authorization rule that determines who is permitted to execute one or more enterprise bean methods.

MHS (message handling system) (n.) A group of connected URL mappings, their user agents, and message stores.

MIB (management information base) (n.) A tree-like structure that defines the variables that the SNMP master agent can access. The MIB provides access to the HTTP server's network configuration, status, and statistics. Using SNMP, you can view this information from the NMS. See also AUTH.

migration (n.) The process of transporting data files, such as data configuration or customization, from one version of a product to another.

MIME (multipurpose internet mail extensions) (n.) An emerging standard for multimedia email and messaging. A protocol you can use to include multimedia in email messages by appending the multimedia file in the message.

MIME data type (n.) MIME types control what types of multimedia files the system supports.

mime.types file (n.) The MIME type configuration file. This file maps file extensions to MIME types to enable the server to determine the type of content being requested. For example, requests for resources with `.html` extensions indicate that the client is requesting an HTML file, while requests for resources with `.gif` extensions indicate that the client is requesting an image file in GIF format.

mirror node (n.) An active HADB node that contains the same data as another active node, but resides in the other data redundancy unit. Each active node must have a mirror node; therefore nodes occur

in pairs. When a node detects that its mirror node has failed, it takes over the failed node's role and continues service. See also HADB, active node, spare node, and data redundancy unit (DRU).

mixed-content model (n.) A DTD specification that defines an element as containing a mixture of text and one more other elements. The specification must start with `#PCDATA`, followed by diverse elements, and must end with the "zero-or-more" asterisk symbol (*).

MMP (Messaging Multiplexor) (n.) A specialized Messaging Server that acts as a single point of connection to multiple mail servers, facilitating the distribution of a large user base across multiple mailbox hosts.

mobile application configuration (n.) An Access Manager service that allows the setup of address book, calendar, and mail applications for delivery to a mobile device.

mobile client type See *client type.

mobile device (n.) A transportable wireless device such as a mobile phone or a personal digital assistant.

mobile devices link (n.) A hypertext link appearing on the Portal Desktop.

mobile devices page (n.) A web page which allows users to manage mobile device options.

Mobile Portal Desktop (n.) A Portal Desktop displayed on a mobile device.

moderator (n.) A person who first receives all email addressed to a mailing list in order to decide if the message should be forwarded to the mailing list. The moderator can edit the message before forwarding the message to the mailing list. See also mail list, expansion, member.

module (1) (n.) See J2EE module.

(2) (n.) A group of Java Enterprise System *servers* dependent on one another or closely enough related to be deployed as a unit to provide a specific service or set of services. Service modules are multi-server assemblies that have been pretested for use in *deployment architectures*.

modutil (n.) Software utility required for installing the PKCS#11 module for external encryption or hardware accelerator devices.

MTA (message transfer agent) (n.) A specialized program for routing and delivering messages. MTAs work together to transfer messages and deliver them to the intended recipient. The MTA determines whether a message is delivered to the local message store or routed to another MTA for remote delivery.

MTA configuration file (n.) The `imta.cnf` file that contains all channel definitions for the Messaging Server as well as the rewrite rule that determine how addresses are rewritten for routing.

MTA directory cache (n.) A snapshot of the directory service information about users and groups required by the MTA to process messages. See also directory synchronization

MTA hop (n.) The act of routing a message from one MTA hop to another.

MUA See user agent.

multihomed host (n.) A host that is on more than one public network.

multihost disk (n.) A disk that is physically connected to multiple nodes.

multimaster replication (n.) A replication model in which entries can be written and updated on any of several master replica copies without requiring communication with other master replicas before the write or update is performed. Each server maintains a change log for the replica. Modifications made on one server are automatically replicated to the other servers. In case of conflict, a time stamp is used to determine which server holds the most recent version.

multiplexor (n.) The server containing the database link that communicates with the remote server.

multipurpose internet mail extensions See MIME.

mutual authentication (n.) An authentication mechanism employed by two parties for the purpose of proving each other's identity to one another.

MX record (mail exchange record) (n.) A type of DNS record that maps one host name to another.

N

n + 1 directory problem (n.) The problem of managing multiple instances of the same information in directories and databases of different types, resulting in increased hardware and personnel costs.

name collision (n.) A conflict that occurs during replication if multiple entries have been added or renamed and there is an attempt to use the same DN. The conflicting entries are renamed automatically by the directory servers to ensure DN uniqueness.

name identifier (n.) The pseudonym used to map a user's account information across a number of service and identity provider organizations in order to preserve anonymity. Through the use of this identifier, neither the identity provider nor the service provider know the user's actual identity.

name resolution (n.) The process of mapping an IP address to the corresponding name. See also DNS.

namespace (1) (n.) The tree structure of an LDAP directory. See also DIT.

(2) (n.) A standard that lets you specify a unique label for the set of element names defined by a DTD. A document using that DTD can be included in any other document without having a conflict between element names. The elements defined in your DTD are then uniquely identified so that, for example, the parser can tell when an element `<name>` should be interpreted according to your DTD rather than using the definition for an element `<name>` in a different DTD.

naming attribute (n.) The final attribute in a DIT distinguished name. See also relative distinguished name.

naming context (1) (n.) A specific suffix of a DIT that is identified by its DN. In Directory Server, specific types of directory information are stored in naming contexts. For example, a naming context that stores all entries for marketing employees who work at the Example Corporation's Boston office might be called `ou=mktg, ou=Boston, o=example, c=US`.

(2) (n.) A set of associations between unique, people-friendly names and resources. See also JNDI extension, JNDI name, resource.

naming environment (n.) A mechanism that allows a component to be customized without the need to access or change the component's source code. A container implements the component's naming environment and provides it to the component as a JNDI naming context. Each component names and accesses its environment entries using the `java:comp/env` JNDI context. The environment entries are declaratively specified in the component's deployment descriptor.

native channel (n.) A Portal Server channel which displays native content.

native content (n.) Content written in a native markup language such as HTML that can be sent to a client without conversion.

native desktop (n.) A Portal Server Desktop that displays native content.

NDN (nondelivery notification) (n.) A nondelivery report that the MTA sends back to the sender (with the original message) if the MTA does not find a match during message transmission between the address and a rewrite rule.

nested role (n.) A role that names other role definitions. The set of members of a nested role is the union of all members of the roles it contains. Nested roles may also define extended scope to include the members of roles in other subtrees.

NetFile (n.) A Java™ technology-based file server application that enables users to have remote access to file systems, thereby enabling remote operations on files and directories.

Netlet (n.) A Java applet used in Java Enterprise System Portal Server to allow any applications based on Transmission Control Protocol/Internet Protocol to securely connect to servers through an authenticated Portal Server connection.

NetMail (n.) The NetMail component implements the NetMail (Java technology-based client) and NetMail Lite email clients. These clients work with standard IMAP and SMTP servers.

Netscape™ Console (n.) An application written in the Java programming language that provides server administrators with a graphical interface for managing all Netscape servers from one central location anywhere within the enterprise network. From any installed instance of Netscape Console, you can see and access all the Netscape servers on the enterprise's network to which you have been granted access rights.

network management station See NMS.

network manager (n.) A program that reads, formats, and displays SNMP data. Also known as an SNMP client.

Network Security Services for Java (JSS) (n.) A class library that provides Java bindings to the Network Security Services SSL library. Portal Server uses this class library to initiate secure socket layer connections from servlets and to accept SSL connections in the Portal Server Secure Remote Access Pack gateway.

news channel (n.) Forums for posting and sharing information. Users subscribe to news channels in order to see updates. The information in a news channel is usually published automatically by way of a URL or published by a user with the proper privilege. Administrators can control news channel access by assigning users to the channels they need and deciding who can see or publish information to news channels.

news channel list (n.) A window that shows all the news channels to which you are currently subscribed. Each news channel is indicated by a separate tab.

next-hop list (n.) A list of adjacent systems that a mail route uses to determine where to transfer a message. The order of the systems in the next-hop list determines the order in which the mail route transfers messages to those systems.

NIS (network information service) (n.) (UNIX only) A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computers.

NMS (network management station) (n.) A powerful workstation with one or more network management applications installed. The NMS is a machine used to remotely manage your network.

NNTP (Network News Transfer Protocol) (n.) A protocol for newsgroups. You must define your news server host to use agent services on your server.

node (1) (n.) A computing node. One of a number of computers in a network or Internet environment. Distributed applications are deployed across this environment, with different distributed components, *business services*, and *servers* running on the various computing nodes. See also cluster.

(2) (n.) See HADB node.

node agent (n.) A lightweight agent that is required on every machine that hosts at least one Application Server server instance, including the machine that hosts the Domain Administration Server. The node agent performs tasks including starting, stopping, creating and deleting Application Server instances as instructed by the Domain Administration Server.

nondelivery notification See NDN.

NoPassword authentication (n.) A type of authentication that allows users to log in to the Access Manager without being prompted for a password.

normalization (n.) The process of removing redundancy by modularizing, as with subroutines, and of removing superfluous differences by reducing them to a common denominator. For example, line endings from different systems are normalized by reducing them to a single new line, and multiple white space characters are normalized to one space.

North American Industry Classification System (NAICS)

(n.) A system for classifying business establishments based on the processes they use to produce goods or services.

NOTARY messages

(n.) Nondelivery notifications (NDNs) and delivery status notifications that conform to the NOTARY specifications RFC 1892.

notation

(n.) A mechanism for defining a data format for a non-XML document referenced as an unparsed entity. This is a holdover from SGML. A newer standard is to use MIME data types and namespaces to prevent naming conflicts.

notification message

(n.) A type of message sent by the Messaging Server providing the status of message delivery processing and the reasons for any delivery problems or outright failures. The messages are for information al purposes and require no action from the postmaster. See also delivery status notification

notification service

(n.) A service that receives subscriptions and notifications from other servers and then relays notifications to specific subscribers. The Calendar Server `csnotifyd` service sends notifications of events and to-do tasks using Event Notification Service (ENS) as the broker for the events.

NSAPI

See server plug-in API.

ns-slapd

(n.) (UNIX only) A process or service responsible for all actions of the Directory Server. On Windows systems, the equivalent is slapd.exe.

ns-slapd.exe

(n.) (Windows only) The process monitor on Windows systems.

O

OASIS (Organization for the Advancement of Structured Information Standards) (n.) A consortium that drives the development, convergence, and adoption of e-business standards. Its Web site is `http://www.oasis-open.org/`. The DTD repository it sponsors is at `http://www.XML.org`.

obj.conf file (n.) The server's object configuration file. This file contains additional initialization information, settings for server customizing, and instructions that the server uses to process requests from clients (such as browsers). Web Server reads this file every time it processes a client request.

object class (n.) A template specifying the kind of object that the entry describes and the set of attributes that entry contains. For example, Directory Server specifies an `emailPerson` object class which has attributes such as `commonname`, `mail` (email address), `mailHost`, and `mailQuota`.

object identifier See OID.

object persistence See persistence.

obsolete patch (n.) A patch no longer considered valid or up-to-date. A patch is considered obsolete when a subsequent version of the patch fixes the same issue, when a different patch includes the fix from the original, or when the patch is no longer considered relevant.

offline state (n.) A state in which the mail client downloads messages from a server system to a client system where they can be viewed and answered. The messages might or might not be deleted from the server.

OID (object identifier) (n.) A string representation of an object identifier which consists of a list of decimal numbers separated by periods (for example, 1.3.6.1.4.1). In Lightweight Directory Access Protocol, object identifiers are used to uniquely identify schema elements, including object classes and attribute types. The top levels of an object identifier hierarchy are managed by standards bodies and are delegated to organizations who wish to construct their own schema definitions.

OMG (Object Management Group) (n.) A consortium that produces and maintains computer industry specifications for interoperable enterprise applications. Its Web site is `http://www.omg.org/`.

one-way messaging (n.) A method of transmitting messages without having to block until a response is received.

online state (n.) A state in which messages remain on the server and are remotely responded to by the mail client.

operational attribute (n.) An operational attribute contains information used internally by the directory to keep track of modifications and subtree properties. Operational attributes are not returned in response to a search unless explicitly requested.

optional attribute list (n.) A list of optional attributes for a specified object class. Optional attributes are preceded by the keyword MAY.

ORB (Object request broker) (n.) A library that enables CORBA objects to locate and communicate with one another.

organization (n.) In Directory Server Access Management Edition, an object that represents the top level of a hierarchical structure used by an enterprise to manage its departments and resources. Upon installation, Directory Server Access Management Edition dynamically creates a top-level organization (`default o=isp`) to manage the Directory Server Access Management Edition enterprise configurations. Additional organizations can be created after installation to manage separate enterprises. All created organizations fall beneath the top-level organization. See also suborganization.

organization administrator (n.) A user who has administrative privileges to create, modify, and delete mail users and mail lists in an organization or suborganization by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs.

O/R mapping tool (object-to-relational database tool) (n.) A mapping tool within the Application Server Administrative interface that creates XML deployment descriptors for entity beans.

OSI tree (Open Systems Interconnect tree) (n.) A DIT that mirrors the Open Systems Interconnect network syntax. An example of a distinguished name (DN) in an OSI tree would be `cn=billt,o=bridge,c=us`.

OS principal (n.) A principal native to the operating system on which the J2EE platform is executing.

OTS (Object Transaction Service) (n.) A definition of the interfaces that permit CORBA objects to participate in transactions.

P

package (n.) A collection of files and directories. Packaging is a method distributing software for installation. See also assembly, deployment.

parameter (1) (n.) A name-value pair sent from the Java Enterprise System Application Server client, including form field data, HTTP header information, and so on, and encapsulated in a request object. See also attribute, property.

(2) (n.) An argument to a Java method or database-prepared command.

parameter entity (n.) An entity that consists of DTD specifications, as distinct from a general entity. A parameter entity defined in the DTD can then be referenced at other points, thereby eliminating the need to recode the definition at each location it is used.

parent (n.) An element in an XML file that contains another element, referred to as a child. See also child.

parent access (n.) When granted, indicates that users have access to entries below their own position in the directory tree if the bind DN is the parent of the targeted entry.

parsed entity (n.) A general entity that contains XML and therefore is parsed when inserted into the XML document, as opposed to an unparsed entity.

parser (n.) A module that reads in XML data from an input source and breaks it into chunks so that your program knows when it is working with a tag, an attribute, or element data. A non-validating parser ensures that the XML data is well formed but does not verify that it is valid. See also validating parser.

partition See message store partition.

passivation (n.) The process of transferring an enterprise bean from memory to secondary storage. A method of releasing a bean's resources from memory without destroying the bean. In this way, a bean is made to be persistent and can be recalled without the overhead of instantiation. See also activation.

pass-through authentication See PTA.

pass-through subtree (n.) In pass-through authentication, the PTA Directory Server passes through bind requests to the authenticating Directory Server from all clients whose DN is contained in this subtree.

password authentication (n.) Identification of a user through user name and password. See also certificate-based authentication.

password file (n.) (UNIX only) A file that stores UNIX user login names, passwords, and user ID numbers. The password file is also known as `/etc/passwd` because of where the file is located.

password policy (n.) A set of rules that govern how passwords are used in a given directory.

patch version number (n.) The last two digits of the patch identifier, for example, "nnnnnn-03". The number is increased by one each tome a new version of the patch is released.

pattern (n.) A string expression used for matching purposes, such as in Allow and Deny filters.

`PCDATA` (n.) A predefined XML tag for parsed character data, in which the normal rules of XML syntax apply, as opposed to character data (`CDATA`), which means "don't interpret these characters." See also `CDATA`.

PDC (personal digital certificate) (n.) An electronic certificate attached to a message that authenticates a user. A personal digital certificate can be created by correctly entering a user ID and password or by using an SSL certificate request that in turn uses the security certificate of the server through which the user is connected.

peer (n.) A subcategory that has the same parent category as another.

permanent failure (n.) An error condition that occurs during message handling. When a permanent failure occurs, the message store deletes its copy of an email message. The MTA bounces the message back to the sender and deletes its copy of the message.

permissions (1) (n.) A set of privileges granted or denied to a user or group. This information includes the user or group name, valid email address or addresses, and how and where email is delivered.

(2) (n.) In the context of access control, the permission states whether access to the directory information is granted or denied and the level of access that is granted or denied. See also access rights.

(3) (n.) The settings that control the access to a calendar. For example, in Calendar Express, permissions include Availability, Invite, Read, Delete, and Modify. Calendar Server administrators set permissions as ACE strings using command-line utilities. See also ACL.

persistence (1) (n.) For components, the protocol for transferring the state between instance variables and an underlying database. See entity bean. See also transience.

(2) (n.) For sessions, the session storage mechanism. See also session, failover, session failover.

persistence manager (n.) The manager responsible for the persistence of an EJB 1.x or 2.x entity bean.

persistent field (n.) A virtual field of an EJB 2.1 entity bean that has container-managed persistence; it is stored in a database.

persistent state (n.) Where the state of an object is kept in persistent storage, usually a database.

personal digital certificate See PDC.

personal folder (n.) A folder that can be read only by the owner. See also shared folder

pk12util (n.) The software utility required to export the certificate and key databases from your internal machine and import them into an external PKCS#11 module.

PKI (public key infrastructure) (n.) Enables the identity of a user to be linked to a browser or mobile device. Wireless PKI refers to certificate-based authentication that occurs on the handset.

plaintext (n.) A method for transmitting data. The definition depends on the context. With secure socket layer, plaintext passwords are encrypted and are therefore not sent as cleartext. With SASL, plaintext passwords are hashed, and only a hash of the password is sent as text.

plaintext authentication See password authentication.

pluggable authentication (n.) A mechanism that allows J2EE applications to use the Java™ Authentication and Authorization Service (JAAS) software from the J2SE™ platform. Developers can plug in their own authentication mechanisms.

plug-in (1) (n.) A code extension to the browser that displays or executes content inside a web page. Plug-ins enable the browser to display page content elements that the browser would otherwise not be able to display.

(2) (n.) An accessory program that can be loaded and then used as part of the overall system. For example, the Calendar Server can use a plug-in to access a non-LDAP directory service.

POA (Portable Object Adapter) (n.) A CORBA standard for building server-side applications that are portable across heterogeneous ORB*s*.

pointer CoS (n.) A pointer class of service which identifies the template entry using the template DN only.

point-to-point delivery model (n.) A model where message producer*s* address message*s* to specific message queue*s* and message consumer*s* extract messages from queues established to hold their messages. A message is delivered to one message consumer only.

policy (1.) (n.) A rule that describes who is authorized to access a specific resource under specific conditions. The rule can be based on groups of users or roles in an organization.

(2) (n.)In Directory Server Access Management Edition, defines rules to help protect an organization's web resources. Policies are assigned to organizations and roles only.

poll (n.) The function in Instant Messaging Server that enables you to ask users for their response to a question. You can send a question and possible answers to selected users, and they respond with their selected answer.

pooling (n.) The process of providing a number of pre-configured resources to improve performance. If a resource is pooled, a component can use an existing instance from the pool rather than instantiating a new one. In the Java Enterprise System Application Server, database connections, servlet instances, and enterprise bean instances can all be pooled.

POP3 (Post Office Protocol Version 3) (n.) A protocol that provides a standard delivery method and that does not require the MTA to have access to a user's mail folders. Not requiring access is an advantage in a networked environment where often the mail client and the message transfer agent are on different computers.

port (n.) The location (socket) to which Transmission Control Protocol/Internet Protocol connections are made. Web servers traditionally use port 80, FTP uses port 21, and telnet uses port 23. Java Enterprise System Portal Server uses special ports, particularly on client systems, to securely communicate through the Portal Server session to servers.

portal (n.) An entry point to a set of resources that an enterprise wants to make available to the portal's users. For some consumer portals, the set of resources includes the entire World Wide Web, but for most enterprises, the set of resources includes information, applications, and other resources that are specific to the relationship between the user and the enterprise. The Portal Server Desktop is the application used to generate the portal in Portal Server.

Portal Desktop (n.) Any one of the desktops generated by Portal Server.

Portal Server (n.) A software product that enables remote users to securely access their organization's network and the network's services over the Internet. Creates a secure Internet portal, providing access to content, applications, and data to any targeted audience, including employees,

business partners, or the general public. Referred to as the core part of the complete Sun Java System Portal Server product solution that is shared among all Portal Server packs.

Portal Server Desktop (n.) Provides the primary end-user interface and a mechanism for extensible content aggregation through the content provider interface (PAPI). Often referred to as "Desktop." The Desktop includes a variety of providers that provide a container hierarchy and the basic building blocks for building some types of channels. The Desktop implements a display profile data storage mechanism on top of a Directory Server Access Management Edition service for storing content provider and channel data. The Desktop also includes an admin console module for editing the display profile and other Desktop service data.

Portal Server Instant Collaboration Pack (n.) A server instant messaging product that includes the server, multiplexor, and Instant Messaging components. Also known as Instant Messaging Server.

Portal Server Pack (n.) A generic term that refers to an add-on product for Portal Server.

portal node (n.) A physical machine that is running Portal Server software or Portal Server Pack software. Also called a host.

port number (n.) A number that specifies an individual Transmission Control Protocol/Internet Protocol application on a host machine. Provides a destination for transmitted data.

post-deployment (n.) A stage of the Java Enterprise System solution life-cycle process in which distributed applications are started up, monitored, tuned to optimize performance, and dynamically upgraded to include new functionality.

postinstallation configuration (n.) Access Manager configuration tasks that you perform after you run the Java Enterprise System installer (often with the Configure Later option). Usually, you perform postinstallation tasks only a few times. For example, you might deploy an additional instance of a product or configure a product for session failover. See also configuration.

postmaster account (n.) An alias for the email group and email addresses that receive system-generated messages from the Messaging Server. The postmaster account must point to a valid mailbox or mailboxes.

Post Office Protocol Version 3 See POP3.

pre-deployment (n.) A stage of the Java Enterprise System solution life-cycle process in which business needs are translated into a deployment scenario: a logical architecture

preferred directory server (n.) A directory server master instance used by Identity Synchronization for Windows to detect and apply changes to user entries. While this server is available, Identity Synchronization for Windows will not communicate with any other directory server masters.

prepared command (n.) A database command in SQL that is precompiled to make repeated execution more efficient. Prepared commands can contain parameters. See also prepared statement.

prepared statement (n.) A class that encapsulates a `QUERY`, `UPDATE`, or `INSERT` statement that is used repeatedly to fetch data. A prepared statement contains at least one prepared command.

presence index (n.) A filtering method which enables efficient searching for entries that contain an attribute of a specified type, regardless of the value of the attribute in the entry.

presentation layout (n.) The format of web page content.

presentation logic (n.) Activities that create a page in an application, including processing a request, generating content in response, and formatting the page for the client. Usually handled by a web application.

preset message (n.) Short messages that can be written and saved as Portal Server Mobile Access mobile preferences for later use with a mobile mail application.

primary data view (n.) One of two Directory Proxy Server data views that makes up a join data view. The primary data view is the authoritative source of entries by default. See also secondary data view.

primary document directory See document root.

primary key (n.) The unique identifier that enables the client to locate a particular EJB 2.1 entity beanwithin a home.

primary key class name (n.) A variable that specifies the fully qualified class name of a bean's primary key. Used for Java Naming and Directory Interface ™ (JNDI) lookups.

principal (n.) The identity assigned to a user as a result of authentication. A principal can acquire a federated identity capable of making decisions, and authenticated actions can be done on its behalf. Examples of principals include an individual user, a group of individuals, a corporation, other legal entities, or a component of the Liberty architecture.

private key See public-key cryptography.

privilege (n.) A type of access right that is granted to a user, a set of users, or a resource. This security attribute does not have the property of uniqueness and can be shared by many principals.

process (1) (n.) A self-contained, fully functional execution environment set up by an operating system. Each instance of an application typically runs in a separate process.

(2) (n.) Execution sequence of an active program. A process is made up of one or more threads.

processing instruction (n.) Information contained in an XML structure that is intended to be interpreted by a specific application.

produce (v.) To pass a message to the client runtime for delivery to a destination.

producer (n.) An object (MessageProducer) created by a session that is used for sending messages to a destination. In the point-to-point delivery model, a producer is a sender (QueueSender). In the publish/subscribe delivery model, a producer is a publisher (TopicPublisher).

production environment (n.) A stage of the application life-cycle process, in which distributed applications are started up, monitored, tuned to optimize performance, and dynamically upgraded to include new functionality.

programmatic security (n.) The process of controlling security explicitly in code rather than allowing the component's container, a bean's container, or a servlet engine, for instance, to handle it. Opposite of declarative security. Programmatic security is useful when declarative security alone is not sufficient to express the security model of an application.

programmer-demarcated transaction See bean-managed transaction.

prolog (n.) The part of an XML document that precedes the XML data. The prolog includes the declaration and an optional DTD.

propagation behavior (n.) The synchronization process between a consumer and a supplier.

property (1) (n.) A single name-value pair that defines the behavior of an application component. See also parameter.

(2) (n.) A name-value pair that modifies an element in an XML file, but that is *not* predefined in the DTD file. Contrast with attribute.

(3) (n.) In the Application Server, a name-value pair that is *not* part of the built-in server configuration. Contrast with attribute.

protocol (1) (n.) A set of rules that describes how devices on a network exchange information.

(2) (n.) A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provider (n.) The programmatic aspect of a channel. Adding configuration data to a provider differentiates it into an instance of a channel. A provider is a Java class and is responsible for converting the content in a file or the output of an application or service into the proper format for a channel. A number of providers are shipped with the Portal Server including a bookmark provider, an application provider, and a notes provider. As the desktop is imaged, each provider

is queried in turn for the content of its associated channel. Some providers are capable of generating multiple channels based upon their configuration.

Examples of content providers include the `UserInfoProvider` and `BookmarkProvider`. Examples of container providers include the `TabContainerProvider` and `SingleContainerProvider`. Examples of leaf providers include the `JSPProvider`, `XMLProvider`, `URLScraperProvider` and `SimpleWebServicesProvider`.

provider federation (n.) A group of service providers who contractually agree to exchange authentication information using an architecture based on the Liberty Alliance Project specifications. See also authentication domain.

provisioning (n.) The process of adding, modifying or deleting entries in the Java Enterprise System Directory Server. These entries include users and groups and domain information.

proxy (1) (n.) The mechanism whereby one system acts on behalf of another system in responding to protocol requests. Proxy systems are used in network management to avoid having to implement full protocol stacks in simple devices, such as modems.

(2) (n.) An intermediary program that makes and services requests on behalf of clients. Proxies act as servers and clients in turn and are used to control the content of various network services. See also reverse proxy.

proxy authorization (n.) A special form of authentication where a client binds to the directory with its own identity but is granted the access rights of another user on a per operation basis. This other user is referred to as the proxy user, and its DN is the proxy DN.

proxy DN (n.) The DN of an entry that has access permissions to the target on which the client application is attempting to perform an operation. Used with proxy authorization

Proxylet (n.) A dynamic proxy server than runs on a client machine to redirect a URL to the SRA Gateway. See also Secure Remote Access (SRA)

PTA (pass-through authentication) (n.) Mechanism by which one Java Enterprise System Directory Server consults another Directory Server to check bind rules.

PTA Directory Server (n.) In pass-through authentication, the PTA Directory Server sends (passes through) bind requests it receives to the authenticating Directory Server.

PTA LDAP URL (n.) In pass-through authentication, the URL that defines the authenticating Directory Server, pass-through subtree or subtrees, and optional parameters.

public folder (n.) A folder with multiple owners that is shared by multiple people who can access it. Depending on the ACLs set for the folder, more than one person can update or administer the folder.

public information directories

(n.) (UNIX only) Directories not inside the document root that are in a UNIX user's home directory or under the user's control, or directories that are under the user's control.

public key

(n.) The encryption key used in public-key encryption.

public-key certificate

(n.) A data structure containing a user's public key, as well as information about the time and date during which the certificate is valid. Used in client-certificate authentication to enable the server, and optionally the client, to authenticate each other. The public key certificate is the digital equivalent of a passport. It is issued by a trusted organization, called a certificate authority, and provides identification for the bearer.

public-key cryptography

An method of encryption. In public-key cryptosystems, everyone has two related complementary keys: a publicly revealed key and a secret key (also known as a private key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the secure channels that a conventional cryptosystem requires. Also known as asymmetric key cryptography.

public-key encryption

(n.) A cryptographic method that uses a two-part key (code) that consists of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt the messages, the recipients use their unpublished private keys known only to them.

public key infrastructure

See PKI.

Public Network Management

(n.) Software that uses fault monitoring and failover to prevent loss of node availability because of single network adapter or cable failure. Public Network Management failover uses sets of network adapters called a network adapter failover group to provide redundant connections between a cluster node and the public network. The fault monitoring and failover capabilities work together to ensure availability of resources.

publish and subscribe delivery model

(n.) A messaging system in which publishers and subscribers are generally anonymous and can dynamically publish or subscribe to a specific node in a content hierarchy, called a topic. The system distributes message*s* arriving from a topic's multiple publishers to its multiple subscribers.

purge a message

(v.) To permanently remove a message that has been deleted and is no longer referenced in user and group folders. The space is then returned to the message store file system. See also delete a message and expunge a message.

Q

QOS (quality of service) (n.) The performance limits you set for a server instance or virtual server. For example, if you are an ISP, you might want to charge different fees for virtual servers depending on how much bandwidth is provided. You can limit the amount of bandwidth and the number of connections.

query string (n.) A component of an HTTP request URL that contains a set of parameters and values that affect the handling of the request.

queue (n.) In the Java Message Service, an object created by an administrator to implement the point-to-point delivery model. A queue is always available to hold messages even when the client that consumes its messages is inactive. A queue is used as an intermediary holding place between producers and consumers. See JMS, point-to-point delivery model.

R

RAF (robot application function) (n.) A function that can be used in robot filter configuration files. User-defined robot application functions are also called plug-in functions. These functions are invoked by directives.

RAM (random access memory) (n.) The physical semiconductor-based memory in a computer.

RAR file (resource adapter archive) (n.) A Java™ archive (JAR) file that contains a resource adapter module, also called a connector module.

RC2 (n.) A variable key-size block cipher by RSA Data Security.

rc.2.d file (n.) (UNIX only) A file on UNIX machines that describes programs that are run when the machine starts. This file is also called `/etc/rc.2.d` because of its location.

RC4 (n.) A stream cipher by RSA Data Security. Faster than RC2.

RD See resource description.

RDB (n.) Relational database.

RDBMS (n.) Relational database management system.

RDF (Resource Description Framework) (n.) A standard for defining the kind of data that an XML file contains. Such information can help ensure semantic integrity, for example, by helping to make sure that a date is treated as a date rather than simply as text.

RDF schema (n.) A standard for specifying consistency rules that apply to the specifications contained in an RDF.

RDM See resource description message.

RDN (relative distinguished name) (n.) The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full DN. Most RDNs consist of a single attribute type and value from the entry.

read-only bean (n.) An entity bean that is never modified by an EJB™ client. See also entity bean.

realm (n.) A scope over which a common security policy is defined and enforced by the security administrator of the security service. Also known as a security policy domain or security domain. In the J2EE server authentication service, a realm is a complete database of roles, users (or principals), and groups that identify valid users of a web application or a set of web applications.

redirection (n.) A mechanism by which clients accessing a particular URL are sent to a different location, either on the same server or on a different server. Redirection is useful if a resource has moved and you want the clients to use the new location transparently. Redirection is also used to maintain the integrity of relative links when directories are accessed without a trailing slash.

reentrant entity bean (n.) An entity bean that can handle multiple simultaneous, interleaved, or nested invocations that will not interfere with each other.

reference (n.) A reference to an entity that is substituted for the reference when the XML document is parsed. See entity reference.

reference deployment architecture (n.) A deployment architecture that has been designed, implemented, and tested for performance. Reference deployment architectures are used as starting points for designing deployment architectures for custom solutions.

referential integrity (n.) The mechanism that ensures that relationships between entries expressed by DN-valued attributes are maintained within the directory.

referral (n.) When a server receives a search or update request from a client that it cannot process, the server sends back to the client a pointer to the Java Enterprise System Directory Server that can process the request.

referral hop limit (n.) The maximum number of referrals that a client should follow in a row.

registry (n.) An infrastructure that enables the building, deployment, and discovery of web services. It is a neutral third party that facilitates dynamic and loosely coupled business-to-business (B2B) interactions.

registry provider (n.) An implementation of a business registry that conforms to a specification for XML registries (for example, ebXML or UDDI).

regular expression (n.) A text string that uses special characters to represent ranges or classes of characters for the purpose of pattern matching.

relative distinguished name See RDN.

relationship field (n.) A virtual field of an entity bean having container-managed persistence; it identifies a related entity bean.

relaying (n.) The process of passing a message from one messaging server to another messaging server.

remote interface (n.) One of two interfaces for EJB 1.x and 2.x components. The remote interface defines the business methods callable by a client. See also home interface.

`remove` **method** (n.) A method defined in the home interface and invoked by a client to destroy an EJB 1.x or 2.x enterprise bean.

renderer (n.) A Java class that can render the output for a set of JavaServer Faces UI component*s*.

rendering (1) (n.) The process of converting content written in Abstract Markup Language (AML) to the appropriate device-specific markup language for a specific mobile device.

(2) (n.) The process of producing output for a client. See renderer.

rendering channel (n.) A Portal Server Mobile Access channel that displays rendering content.

rendering engine (n.) In Portal Server, converts AML to the language appropriate for a given mobile client.

rendering filter (n.) The filter that passes content for conversion between the rendering engine and client.

render kit (n.) A set of renderers that render output to a particular client. The JavaServer Faces technologyimplementation provides a standard HTML render kit, which is composed of renderers that can render HTML markup.

replica (n.) A suffix on a directory server that is linked to one or more other suffixes through a replication agreement.

replica cycle See replication cycle.

replica directory server (n.) The directory that receives a copy of all or part of the data.

replica group (n.) The servers that hold instances of a particular area of replication. A server can be part of several replica groups.

replication (n.) The process of synchronizing data distributed across Directory Servers and rectifying update conflicts.

replication agreement (n.) A set of configuration parameters that are stored on the supplier server and that identify the suffixes to replicate, the consumer servers to which the data is pushed, the times during which replication can occur, the DN and credentials used by the supplier to bind to the consumer, and how the connection is secured.

replication base entry (n.) The DN of the root of a replicated area.

replication cycle (n.) The interval during which update information is exchanged between two or more replicas. The replication cycle begins during an attempt to push data to or pull data from another replica or set of replicas and ends when the data has successfully been exchanged or when an error is encountered.

replication session (n.) A session set up between two servers in a replica group to pass update information as part of a replication cycle.

request object (n.) An object that contains page and session data produced by a client, passed as an input parameter to a servlet or a page created with the JavaServer Pages technology

request-response messaging (n.) A method of messaging that includes blocking until a response is received.

required attribute list (n.) A list of required attributes for a specified object class. Required attributes are preceded by the keyword MUST.

required attributes (n.) Attributes that must be present in entries using a particular object class. See also allowed attributes, attribute.

resource (1) (n.) Any item on a network that can be identified by a URL, such as a web page, a document, or an FTP directory. A resource is often referred to informally as a document.

(2) (n.) Any URL, directory, or program that the server can access and send to a client that requests it.

(3) (n.) A program object that provides connections to systems, such as database servers and messaging systems.

resource adapter (n.) A system-level software driver that is used by an EJB container or an application client to connect to an enterprise information system (EIS). A resource adapter typically is specific to an EIS. It is available as a library and is used within the address space of the server or client using it. A resource adapter plugs in to a container. The application components deployed on the container then use the client API (exposed by the adapter) or tool-generated high-level

abstractions to access the underlying EIS. The resource adapter and EJB container collaborate to provide the underlying mechanisms-transactions, security, and connection pooling-for connectivity to the EIS. See also connector.

resource adapter module (n.) A deployable unit that contains all Java interfaces, classes, and native libraries, implementing a resource adapter along with the resource adapter deployment descriptor.

resource calendar (n.) A calendar associated with a resource such as a meeting room or equipment such as a notebook computer or overhead projector.

resource description (n.) A list of attribute-value pairs associated with a resource through a URL. Agents can generate resource descriptions automatically or people can write resource descriptions manually. Once a repository of resource descriptions is assembled, the server can export the repository through resource description messages as a programmatic way for web agents to discover and retrieve the resource descriptions. Resource descriptions are stored in SOIF format.

resource description message (n.) A mechanism to discover and retrieve metadata about network-accessible resources, known as resource descriptions.

resource invocation (n.) An instance of a resource type running on a node. An abstract concept representing a resource that was started on the node.

resource manager (n.) Provides access to a set of shared resources. A resource manager participates in transactions that are externally controlled and coordinated by a transaction manager. A resource manager typically is in a different address space or on a different machine from the clients that access it. Note: An enterprise information system (EIS) is referred to as a resource manager when it is mentioned in the context of resource and transaction management.

resource manager connection (n.) An object that represents a session with a resource manager.

resource manager connection factory (n.) An object used for creating a resource manager connection.

resource offering (n.) In a Discovery Service, a resource offering defines associations between a piece of identity data and the service instance that provides access to it.

resource reference (n.) An element in a deployment descriptor that identifies the component's coded name for the resource.

response buffer (n.) The Portal Server Mobile Access server response buffer stores large responses as separate smaller responses so that they fit limited device buffers.

response object (n.) An object that references the calling client and provides methods for generating output for the client.

restart (v.) To start the robot without deleting its state information, which causes the robot to start running in the same state in which it previously stopped. Opposite of a fresh start.

restore (v.) To copy the contents of folders from a backup device to the message store. See also back up.

ResultSet object (n.) An object that implements the `java.sql.ResultSet` interface. `ResultSet` objects are used to encapsulate a set of rows retrieved from a database or other source of tabular data.

resync interval (n.) How often a connector checks a Identity Synchronization for Windows directory source for changes. This periodic check is efficient and only requires reading entries of users that have changed since the last check. The console expresses this value in milliseconds and provides 1000 (1 second) as a default.

retro changelog (n.) Stores changes in the order of arrival on the local server and not in the order in which these changes were applied to the system. The retro changelog was not designed to function in a multimaster replication environment. Not the same as change log, as the retro changelog is not used in replication. Provides backward compatibility with Directory Server 4.

reusable component (n.) A component created so that it can be used in more than one capacity, for example, by more than one resource or application.

reverse DNS lookup (n.) The process of querying the DNS to resolve a numeric IP address into the equivalent gateway.

reverse proxy (n.) A proxy that performs bidirectional URL rewriting and translation between clients and servers. Unlike a proxy, which exists at the client side, a reverse proxy exists at the server side of the network. In Java Enterprise System Portal Server, the reverse proxy exists in Java Enterprise System Portal Server Secure Remote Access Pack.

Rewriter (n.) The Rewriter provides a Java class library for rewriting URL references in various web languages, such as HTML, Javascript, and XML, and in HTTP location headers (redirections). The Rewriter defines a Java Enterprise System Directory Server Access Management Edition service for storing rules that define how rewriting is to be done and the data to be rewritten. The Rewriter also includes an admin console module for editing these rules.

rewrite rule (n.) A tool that the MTA uses to route messages to the correct host for delivery. Rewrite rules perform the following functions: (1) extract the host and domain specification from an address of an incoming message, (2) match the host and domain specification with a rewrite rule pattern, (3) rewrite the host and domain specification based on the domain template, and (4) decide which channel queue the message should be placed in. Also known as a domain rewrite rule.

RFC (request for comments) (n.) A document series maintained by the Internet Engineering Task Force that describes the Internet suite of protocols and related experiments. Very few RFCs describe Internet standards, but all Internet standards are published as RFCs. See http://www.imc.org/rfcs.html.

RMI (remote method invocation) (n.) A technology that allows an object running in one Java virtual machine to invoke methods on an object running in a different Java virtual machine.

RMI-IIOP (n.) A version of RMI implemented to use the CORBA IIOP protocol. RMI over IIOP provides interoperability with CORBA objects implemented in any language if all the remote interfaces are originally defined as RMI interfaces.

RMIC (n.) remote method invocation compiler.

robot (n.) A program that finds all the resources located in a specific portion of a network.

robot application function See RAF.

role (1) (n.) An abstract logical grouping of users that is defined by the application assembler. When an application is deployed, the roles are mapped to security identities, such as users (principals) or groups, in the operational environment. See also user, group.

(2) (n.) In the J2EE server authentication service, an abstract name for permission to access a particular set of resources.

(3) (n.) In Java Enterprise System Directory Server Access Management Edition, a grouping that represents a selection of privileged operations. By applying the role to a user or a service, the principal can perform the operations. For example, by confining certain privileges to an Employee role or a Manager role and applying the role to a user, the user's accessibility is confined to the privileges granted to it by the role. Roles are defined using access control instructions (ACIs).

(4) (n.) The function performed by a party in the development and deployment phases of an application developed using J2EE technology. The roles are application component provider, application assembler, deployer, J2EE product provider, EJB container provider, EJB server provider, Web container provider, Web server provider, tool provider, and system administrator.

role-based attributes (n.) Attributes that appear on an entry because the entry possesses a particular role within an associated CoS template.

role mapping (n.) The process of associating the groups or principals (or both), recognized by the container with security roles specified in the deployment descriptor. Security roles must be mapped by the deployer before a component is installed in the server.

rollback (n.) Cancellation of a transaction. The point in a transaction when all updates to any resources involved in the transaction are reversed.

root (1) (n.) (UNIX only) The most privileged user on UNIX machines. The root user has complete access privileges to all files on the machine.

(2) (n.) The outermost element in an XML document. The element that contains all other elements.

root DN (n.) The DN of the Directory Manager.

Root DSE (n.) An entry that is automatically generated by the Directory Server and is returned from a `baseObject` search with a DN that is empty (zero bytes long). The Root DSE provides information to clients about the server\qs configuration, such as a pointer to the subschema entry, a list of the DNs of the naming contexts held by the server, and a list of the LDAPv3 controls and extensions that the server supports. See also DSE.

root entry (n.) The top-level entry of the DIT hierarchy.

root suffix (n.) The parent of one or more sub suffix. A directory tree can contain more than one root suffix.

router (n.) A system responsible for determining on which path network traffic will flow. A router uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as a "routing matrix." In Open Systems Interconnect terminology, a router is a Network Layer intermediate system. See also gateway.

routing See message routing.

routing tables (n.) The internal databases that hold the information about message originators and recipients.

row (n.) A single data record that contains values for each column in a table.

RowSet object (n.) An object that encapsulates a set of rows retrieved from a database or other source of tabular data. The `RowSet` object extends the `java.sql.ResultSet` interface, enabling the ResultSet object to act as a component based on the JavaBeans™ component architecture.

RPC (remote procedure call) (n.) A mechanism for accessing a remote object or service.

RTT (round trip time) (n.) The elapsed time for transit of a signal over a closed circuit (from the server to the client and back). This delay is important in systems that require two-way interactive communication where the RTT directly affects the throughput rate. In the context of Java Enterprise System Directory Server, the RTT and the TCP window can have a significant impact on replication performance over a wide-area network. Also known as **round-trip delay time**.

rules (n.) Logical tests applied to determine whether a condition is met. The robot uses rules as part of filters for determining types of content to index and in classification rules to determine what category to assign to a resource.

S

SAAJ (SOAP with Attachments API for Java) (n.) The basic package for SOAP messaging, SAAJ contains the API for creating and populating a SOAP message.

SAF (server application function) (n.) A function that participates in request processing and other server activities.

safe file system (n.) A file system that performs logging so that if a system crashes the system can roll back the data to a pre-crash state and restore all data. An example of a safe file system is Veritas File System, VxFS.

SASL (simple authentication and security layer) (n.) A means for controlling the mechanisms by which POP, IMAP or SMTP clients identify themselves to the server. Java Enterprise System Messaging Server support for SMTP SASL use complies with RFC 2554 (ESMTP AUTH). SASL is defined in RFC 2222. See also POP3 and IMAP4.

SAX (Simple API for XML) (n.) An event-driven interface in which the parser invokes one of several methods supplied by the caller when a parsing event occurs. Events include recognizing an XML tag, finding an error, encountering a reference to an external entity, or processing a DTD specification.

schema (1) (n.) Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

(2) (n.) The structure of the tables and columns in a database. In the Application Server, a schema can be automatically generated from an entity bean.

(3) (n.) A database-inspired method for specifying constraints on XML documents using an XML-based language. Schemas address deficiencies in DTD files, such as the inability to put constraints on the kinds of data that can occur in a particular field. Because schemas are

founded on XML, they are hierarchical. Thus it is easier to create an unambiguous specification, and it is possible to determine the scope over which a comment is meant to apply.

schema checking (n.) A verification process which ensures that entries added or modified in the directory conform to the defined schema. Schema checking is on by default and users receive an error if they try to save an entry that does not conform to the schema.

schema name (n.) The schema or type of a SOIF. For example, a SOIF for a document has the schema name `@DOCUMENT`, while a SOIF for a resource description message header has the schema name `@RDMHeader`.

SCM See service control manager.

scoping (n.) Restrictions placed on the resource descriptions imported by an import agent. The syntax used is the same as that for user searches.

search base See base DN.

Search database (n.) A searchable database of resource descriptions usually generated by a robot. See also robot.

search data hiding rule (n.) A rule that determines how Directory Proxy Server should filter and return the result of a search operation to a client.

Search Engine (n.) A search feature incorporated into Portal Server 6.0. Previously called Compass Server (Portal Server 3.0). The Search Server holds a database of resource descriptions gathered by robots, usually categorized. Users can search the resource descriptions or browse through the categories to locate particular resources.

secondary data view (n.) One of two Directory Proxy Server data views that makes up a join data view. The secondary data view generally provides additional information about entries in the primary data view. See also primary data view.

secondary directory server (n.) A master directory server master instance in multimaster replication environment that Identity Synchronization for Windows can use when the preferred directory server is not available. While the preferred directory server is unavailable, Identity Synchronization for Windows can synchronize changes made in Active Directory or Windows NT to the secondary directory server, but changes made at the secondary server or any other directory server master will not be synchronized until the preferred directory server is available.

Secure Remote Access (SRA) (n.) SRA allows most client devices access to personalized portal applications, content, files and services through a secure connection. Also called Sun Java™ System Portal Secure Remote Access (SRA).

secure socket layer See SSL.

security (n.) A screening mechanism that ensures that application resources are only accessed by authorized clients.

security attribute (n.) An attribute associated with a principal. Security attributes can be associated with a principal by an authentication protocol or by a J2EE product provider or both.

security constraint (n.) A declarative way to annotate the intended protection of web content. A security constraint consists of a web resource collection, an authorization constraint, and a user data constraint.

security context (n.) An object that encapsulates the shared state information regarding security between two entities.

security-module database (n.) A file that contains information describing hardware accelerators for SSL ciphers. Also called `secmod`.

security permission (n.) A mechanism defined by J2SE, and used by the J2EE platform to express the programming restrictions imposed on application component developers.

security permission set (n.) The minimum set of security permissions that a J2EE product provider must provide for the execution of each component type.

security policy domain See realm.

security role See role.

security technology domain (n.) A scope over which the same security mechanism is used to enforce a security policy. Multiple security policy domains can exist within a single technology domain.

security view (n.) The set of security roles defined by the application assembler.

self access (n.) When granted, indicates that users have access to their own entries if the bind DN matches the targeted entry.

self-generated certificate (n.) Public key value only used when entities are named using the message digest of their public value and when these names are securely communicated. See also issued certificate.

sendmail (n.) (UNIX only) A common MTA. In most applications, Java Enterprise System Messaging Server can be used as a drop-in replacement for sendmail.

serializable object (n.) An object that can be deconstructed and reconstructed, which enables it to be stored or distributed among multiple servers.

server (n.) A multi-threaded software process (as distinguished from a hardware server) that provides a distributed or cohesive set of services for clients that access the service by way of an external interface.

server administrator (n.) The person who performs server management tasks. The server administrator provides restricted access to tasks for a particular server, depending upon task ACIs. The configuration administrator must assign user access to a server. Once a user has server access permissions, that user is a server administrator who can provide server access permissions to users.

server assembly (n.) A group of Java Enterprise System servers dependent on one another or closely enough related to be installed or deployed as a unit.

server authentication (n.) A method of authentication which allows a client to make sure that it is connected to a secure server, preventing another computer from impersonating the server or attempting to appear secure when the server is not secure.

server certificate (n.) Used with the HTTPS protocol to authenticate web applications. The certificate can be self-signed or approved by a certificate authority (CA). The HTTPS service of the Application Server will not run unless a server certificate has been installed.

server daemon (n.) A process when running that listens for and accepts requests from clients.

server farm (n.) In Web Server, a server farm is a network of one or more nodes running different configurations. In contrast, a cluster is a network of nodes running with identical configurations and web applications.

server instance (1) (n.) An Application Server can contain multiple instances in the same installation on the same machine. Each instance has its own directory structure, configuration, and deployed applications. Each instance can also contain multiple virtual servers. See also virtual server.

(2) (n.) An instance of Directory Server or Directory Proxy Server. An instance is defined by an instance path, and has related database and configuration files. Multiple instances can be run on a single host system.

Server Message Block protocol (n.) A protocol that provides a method for client applications in a computer to read and write to files on and to request services from server programs in a computer network. The SMB protocol can be used over the Internet on top of its Transmission Control Protocol or on top of other network protocols such as Internetwork Packet Exchange and NetBEUI. Java Enterprise System Portal Server uses SMB for NetFile.

server plug-in API (n.) An extension that allows you to extend and customize the core functionality of Java Enterprise System servers and provide a scalable, efficient mechanism for building interfaces between the HTTP server and back-end applications. Also known as NSAPI.

server principal (n.) The operating system principal that the server is executing as.

server process (n.) A self-contained, fully functional execution environment set up by an operating system. Each instance of an application typically runs in a separate process.

server root (1) (n.) A directory on the server machine dedicated to holding the server program and configuration files, maintenance files, and information files. Also known as ServerRoot or the domain directory.

(2) (n.) A directory location relative to other files on a server. For example, the default Calendar Server installation for Solaris systems uses the path `/opt/SUNWics5/` as the server root.

(3) (n.) The directory into which all Java Enterprise System servers associated with a given Java Enterprise System Administration Server on a given host are installed. See also installation directory and instance directory.

server-side rules (n.) A set of rules for enabling server-side filtering of mail. Based on the Sieve mail filtering language.

service (1) (n.) A function provided by a server. For example, Java Enterprise System Messaging Server provides SMTP, POP, IMAP, and HTTP services.

(2) (n.) A software function performed for one or more clients. This function might be at a very low level, such as a memory management, or at a high level, such as a credit check business service. A high-level service can consist of a family of individual services. Services can be local (available to local clients) or distributed (available to remote clients).

service control manager (n.) (Windows NT only) An administrative program for managing services.

service element (n.) A representation of the combination of one or more connector components that share a single engine component for processing incoming requests.

service endpoint interface (n.) A Java interface that declares the methods that a client can invoke on a web service.

service quality component (n.) One of a number of kinds of system component*s* included in Java Enterprise System. Support components, which include access components and administrative components, provide support for system service

service-oriented architecture See SOA.

service provider (n.) Commercial or not-for-profit organizations that offer web-based services. Can include internet portals, retailers, transportation providers, financial institutions, entertainment companies, libraries, universities, and governmental agencies.

Service Registry (n.) The ebXML registry product included in Java Enterprise System.

service stack (n.) A layering of distributed services that are needed to support distributed enterprise applications. The layering reflects the dependency of higher-level services on the services below them in the stack.

servlet (1) (n.) A server-side program written in the Java programming language that extends the functionality of a Web server, generating dynamic content and interacting with Web applications using a request-response paradigm. Servlets are similar to applets in that they run on the server-side, but servlets do not use a user interface.

(2) (n.) An instance of the `Servlet` class. A servlet is a reusable application that runs on a server. In the Java Enterprise System Application Server, a servlet acts as the central dispatcher for each interaction in an application by performing presentation logic, invoking business logic, and invoking or performing presentation layout.

servlet container (n.) A container that provides the network services over which requests and responses are sent, decodes requests, and formats responses. All servlet containers must support HTTP as a protocol for requests and responses but can also support additional request-response protocols, such as HTTPS.

servlet container, distributed (n.) A servlet container that can run a web application that is tagged as distributable and that executes across multiple Java virtual machines running on the same host or on different hosts.

servlet context (n.) An object that contains a servlet's view of the web application within which the servlet is running. Using the context, a servlet can log events, obtain URL references to resources, and set and store attributes that other servlets in the context can use.

servlet engine (n.) An internal object that handles all servlet metafunctions. Collectively, a set of processes that provide services for a servlet, including instantiation and execution.

servlet mapping (n.) Defines an association between a URL pattern and a servlet. The mapping is used to map requests to servlets.

servlet runner (n.) The part of the servlet engine that invokes a servlet with a request object and a response object. See session bean.

session (1) (n.) An object used by a servlet or stateful session bean to track a user's interaction with a J2EE or web application across multiple HTTP requests. See also persistence.

(2) (n.) An instance of a client-server connection. See also client-server model

(3) (n.) For Java Enterprise System Portal Server, a sequence of interactions between a user and one or more applications, starting with login and ending with logout or timeout.

(4) (n.) For Message Queue, a single threaded context for sending and receiving messages. This can be a queue session or a topic session.

session bean (n.) An enterprise bean that is created by a client and usually exists for the duration of a single client-server session only. A session bean performs operations for the client, such as calculations or accessing other enterprise beans. While a session bean can be transactional, a session bean is not recoverable if a system crash occurs. Session bean objects can be either stateless (not associated with a particular client) or stateful (associated with a particular client), so they can maintain conversational state across methods and transactions. See also stateful session bean.

session cookie (n.) A cookie that is returned to the client containing a user session identifier. See also sticky cookie.

session failover (n.) A failover implementation in Access Manager that uses Sun Java System Message Queue as the communications broker and the Berkeley DB as the session store database. This implementation does not use any web container session management facilities. Access Manager session failover retains a user's authenticated session state in the event of a single hardware or software failure, which allows the user's session to fail over to a secondary Access Manager instance without losing any session information or requiring the user to log in again. See also failover, persistence.

session key (n.) A common cryptographic technique to encrypt each individual conversation between two people with a separate key.

session timeout (n.) A specified duration after which a sever can invalidate a user session.

SGML (Standard Generalized Markup Language) (n.) The parent of both HTML and XML. Although HTML shares SGML's propensity for embedding presentation information in the markup, XML is a standard that allows information content to be totally separated from the mechanisms for rendering that content.

shared component (n.) One of a number of kinds of system component*s* included in Java Enterprise System. Shared components, usually libraries, provide local services to other system components. By contrast, a system service provides distributed infrastructure services to other system components (or to application component*s*).

shared component descriptor file (n.) A file containing metadata for a given shared component (usually in XML format).

shared folder (n.) A folder that can be read by more than one person. Shared folders have an owner who can specify read access to the folder and who can delete messages from the shared folder. The shared folder can also have a moderator who can edit, block, or forward incoming messages. Only IMAP folders can be shared. See also personal folder, public folder.

shared-key cryptography (n.) A type of cryptography where each party must have the same key to encrypt or decrypt ciphertext. Also known as symmetric key cryptography.

SHTML (server-side include Hypertext markup language) (n.) An HTML file that includes embedded server-side includes (SSIs).

Sieve (n.) A proposed language for filtering mail.

Simple API for XML See SAX.

simple authentication and security layer See SASL.

simple index (n.) A type of directory listing that displays only the names of the files without any graphical elements. The opposite of fancy indexing.

Simple Mail Transfer Protocol See SMTP.

Simple Network Management Protocol See SNMP.

Simple Object Access Protocol See SOAP.

SIMS (n.) Solstice Internet Mail Server™ and Sun Internet Mail Server™.

single field substitution string (n.) In a rewrite rule, part of the domain template that dynamically rewrites the specified address token of the host and domain address. See also domain template.

single identity (n.) An identity that a user has by virtue of a single user entry in a Java Enterprise System directory. Based on this single user entry a user can be allowed access to various Java Enterprise System resources, such as a portal, web pages, and services such as messaging, calendar, and instant messaging.

single logout (n.) The ability of a user to log out from an identity provider or a service provider, and to be logged out from all service providers or identity providers in that authentication domain.

single sign-on (SSO) (1) (n.) A feature that allows a user's authentication to one service in a distributed system to be automatically applied to other services in the system.

(2) (n.) A situation where a user's authentication state can be shared across multiple J2EE applications in a single virtual server instance. See SSO.

(3) (n.) The authentication process established when a user with a federated identity authenticates to an identity provider. Because the user has a federated identity, the user can access affiliated service providers without having to reauthenticate.

site (n.) A location on the network where the robot goes to look for resources. You determine the address of the site and the kinds of documents you want to index there in a site definition.

site configuration (n.) A capability that provides a simplified configuration allowing Access Manager clients to communicate with multiple load-balanced Access Manager instances. Site configuration supports deployments with multiple load balancers and firewalls around each site.

site definition (n.) Constraints placed on where a robot can go to locate resources. Using site definitions, you can limit a robot to a particular server, a specified group of servers, or a domain. A site definition includes filters that describe what types of documents the robot should index from the site.

SIZE (n.) An SMTP extension enabling a client to declare the size of a particular message to a server. The server might indicate to the client that it is or is not willing to accept the message based on the declared message size. The server can declare the maximum message size it is willing to accept to a client. Defined in RFC 1870.

slapd.exe (n.) (Windows only) The process or service responsible for all actions of the Directory Server. On UNIX systems, the equivalent is ns-slapd.

slave channel program (n.) A channel program that accepts transfers initiated by a remote system. See also master channel program.

smart host (n.) The mail server in a domain to which other mail servers forward messages if they do not recognize the recipients.

SMB protocol See Server Message Block protocol.

SMTP (Simple Mail Transfer Protocol) (n.) The email protocol most commonly used by the Internet and the protocol supported by the Java Enterprise System Messaging Server. Defined in RFC 821, with associated message format descriptions in RFC 822.

SMTP AUTH See AUTH.

SMTP proxy (n.) A variant of SMTP that sends messages from one computer to another on a network and is used on the Internet to route email.

sn attribute (n.) LDAP alias for surname.

SNMP (Simple Network Management Protocol) (n.) A protocol used to exchange data about network activity. With SNMP, data travels between a managed device (anything that runs SNMP such as hosts, routers, your web server, and other servers on your network) and an NMS.

SNMP master agent (n.) Software that exchanges information between the various subagents and the NMS.

SNMP SOCKS (n.) Firewall software that establishes a connection from inside a firewall to the outside when direct connection would otherwise be prevented by the firewall software or hardware, for example, the router configuration.

SNMP subagent (n.) Software that gathers information about the managed device and passes the information to the master agent.

SOA (service-oriented architecture) (n.) Describes a composite application made up of consumers and providers of services. The consumers and providers can exchange messages without reference to one another's concrete location. The architecture also isolates the core processes of an application from other service providers and consumers.

SOAP (Simple Object Access Protocol) (n.) A lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.

SOAP with Attachments API for Java See SAAJ.

soft restart (n.) A way to restart the server that causes the server to internally restart by rereading its configuration files. A soft restart sends the process the `HUP` signal (signal number one). The process itself does not die, as it does in a hard restart.

SOIF (summary object interchange format) (n.) A syntax for transmitting resource descriptions and other kinds of structured objects. Each resource description is represented as a list of attribute-value pairs. SOIF handles both textual and binary data as values and with some minor extensions multi-valued attributes. SOIF is a streaming format that allows bulk transfer of many resource descriptions in a single, efficient stream.

SOIF attribute (n.) A type of data base attribute. Each resource description in the search database has multiple attributes or fields. These attributes are known as SOIF attributes.

Solaris™ logical name (n.) The name typically used to manage Solaris Operating System devices. For disks, these usually look something like `/dev/rdsk/c0t2d0s2`. For each Solaris logical device name, there is an underlying Solaris physical device name. See also Solaris physical name.

Solaris physical name (n.) The name that is given to a device by its device driver in the Solaris Operating System. The name shows up on a Solaris machine as a path under the `/devices` tree. For example, a typical SI disk has a Solaris physical name similar to `devices/sbus@1f,0/SUNW,fas@e,8800000/sd@6,0:c,raw`. See also Solaris logical name.

solution life cycle (n.) A tool for planning and tracking a deployment project. The life cycle structures the preparation, analysis, and design necessary for successful deployment planning into a series of ordered phases. Each phase consists of related tasks that result in outputs that are carried

forward as inputs to subsequent phases. The tasks within each phase are iterative, requiring thorough analysis and design before generating the outputs for that phase.

spare node (n.) An HADB node that can replace a failed active node. If an active node fails, a spare node copies data from the mirror node and becomes active. See also HADB node,active node, mirror node, and data redundancy unit.

spider See robot.

spoofing (n.) A form of network attack in which a client attempting to access or send a message to a server misrepresents its host name.

SQL (structured query language) (n.) The standardized relational database language for defining database objects and manipulating data. SQL2 and SQL3 designate versions of the language.

SQL/J (n.) A set of standards that includes specifications for embedding SQL statements in methods in the Java programming language and specifications for calling Java static methods as SQL stored procedures and user-defined functions. An SQL checker can detect errors in static SQL statements at program development time, rather than at execution time as with a JDBC driver.

SSL (secure socket layer) (n.) A form of secure, low-level encryption that is used by other protocols like HTTP and FTP. The SSL protocol includes provisions for server authentication, encryption of data in transit, and optional client authentication. The protocol allows client-server applications to communicate in a way that cannot be eavesdropped upon or tampered with.

SSL authentication (n.) A method of authentication which confirms users' identities with security certificates by using the information in the client certificate as proof of identity, or verifying a client certificate published in an LDAP directory.

SSL certificate (n.) An electronic token that means you or a vendor have given approval to encrypt and decrypt your secure transactions using PKI. You create a self-signed SSL Certificate when you install Java Enterprise System Portal Server software. However, you can also obtain an SSL Certificate from a certificate vendor who authorizes secure communications services over the Internet.

SSO See single sign-on (SSO).

SSR See server root.

standard index (n.) Indexes that are maintained by default.

starting points (n.) The list of sites that a Search Engine robot visits to begin enumeration of resources.

state (1) (n.) The circumstances or condition of an entity at any given time.

(2) (n.) A distributed data storage mechanism that you can use to store the state of an application using the Java Enterprise System Application Server feature interface `IState2`. See also conversational state, persistent state.

stateful session bean (n.) A session bean that represents a session with a particular client and which automatically maintains conversational state across multiple client-invoked methods.

stateless session bean (n.) A session bean that represents a stateless service. A stateless session bean is completely transient and encapsulates a temporary piece of business logic needed by a specific client for a limited time span. All instances of a stateless session bean are identical.

static group (n.) A mail group defined statically by enumerating each group member. See also dynamic group.

static web content (n.) Static HTML files, images, applet Java archive (JAR) files, and anything else that can be served up directly by the web server without using the Java web container. For Java Enterprise System Portal Server, the web files are installed in the web server (same place as dynamic web application).

status event (n.) Status of a user including whether online.

sticky cookie (n.) A cookie that is returned to the client to force the client to always connect to the same server process. See also session cookie.

sticky load balancing (n.) A method of load balancing where an initial client request is load balanced, but subsequent requests are directed to the same process as the initial request.

stop word (n.) A word identified to the search function as a word on which the search function should not search, for example, words such as "the," "a," "an," and "and." Also known as a drop word.

stored procedure (n.) A block of statements written in SQL and stored in a database. You can use stored procedures to perform any type of database operation, such as modifying records, inserting records, or deleting records. The use of stored procedures improves database performance by reducing the amount of information that is sent over a network.

streaming (n.) A technique for managing how data is communicated through HTTP. When results are streamed, the first portion of the data is available for use immediately. When results are not streamed, the whole result must be received before any part of it can be used. Streaming provides a way to allow large amounts of data to be returned in a more efficient way, improving the perceived performance of the application.

strftime function (n.) A function that converts a date and a time to a string. This function is used by the server when appending trailers. The `strftime` function has a special format language for the date and time that the server can use in a trailer to illustrate a file's last-modified date.

subagent See SNMP subagent.

subdomain (n.) The next-to-last part of a gateway that identifies the division or department within a company or organization that owns the domain name (for example, `support.example.com` and `sales.example.com`). A subdomain is not always specified.

subnet (n.) The portion of an IP address that identifies a block of host IDs.

subordinate reference (n.) The naming context that is a child of the naming context held by your directory server. See also knowledge information.

suborganization (n.) In Java Enterprise System Directory Server Access Management Edition, an object created under an organization and used by an enterprise for more granular control of its departments and resources. For example, when setting up your Java Enterprise System Portal Server, you might create a suborganization called `mycompany` under the top-level object `isp`.

subschema entry (n.) An entry containing all the schema definitions (definitions of object classes, attributes, matching rules, and so on) used by entries in part of a directory tree.

substring index (n.) A search filer which allows for efficient searching against substrings within entries. Substring indexes are limited to a maximum of three characters per index key.

sub suffix (n.) A branch underneath a root suffix.

suffix (n.) The name of the entry in the directory tree below which data is stored. Multiple suffixes are possible within the same directory. Each database only has one suffix.

summary object interchange format See SOIF.

Sun™ Cluster software The Sun Cluster software system that is used to create highly available and scalable services.

Sun Java System Application Server See Application Server.

Sun Java System Communications Express See Communications Express.

Sun Java System Compass Server See Compass Server.

Sun Java System Connector for Microsoft Outlook See Connector for Microsoft Outlook.

Sun Java System Delegated Administrator See Delegated Administrator.

Sun Java System Directory Server See Directory Server.

Sun Java System Instant Messaging Client See Instant Messaging Client.

Sun Java System Message Queue See Message Queue.

Sun Java System Portal Secure Remote Access (SRA) See Secure Remote Access (SRA).

Java System Portal Server See Portal Server.

Sun Java System Synchronization (n.) Software that runs on a Microsoft Windows personal computer and enables users to synchronize calendar events and tasks with mobile devices and personal information managers (PIMs) such as Microsoft Outlook.

Sun Java System Web Server See Web Server.

supplier (n.) A server containing the master copy of directory trees or subtrees that are replicated to consumer servers.

supplier replica (n.) A replica that contains a master copy of directory information and can be updated. A server can hold any number of master replicas.

supplier directory server (n.) Any directory server that sends changes to other directory servers. See also consumer directory server.

symlinks (n.) (UNIX only) A special file or directory that points to another file or directory so that both files or directories have the same contents.

symmetric encryption (n.) Encryption that uses the same key for both encrypting and decrypting. The Data Encryption Standard (DES) is an example of a symmetric encryption algorithm.

symmetric key cryptography See shared-key cryptography.

synchronization (1) (n.) The update of data by a master directory server to a replica directory server.

(2) (n.) The update of the MTA directory cache.

Synchronization User List (n.) Defines users in the Sun and Windows directories to be synchronized. A Synchronization User List can restrict the scope of users to be synchronized based on an LDAP base DN or filter.

system component (n.) Any software package or set of packages included in the Java Enterprise System and installed by the Java Enterprise System installer. There are several kinds of system components: servers that provide distributed infrastructure services, system services which support the system services components by providing access and administrative services, and shared components that provide local services to other system components.

system index (n.) An index that cannot be deleted or modified as it is essential to Directory Server operations.

system service (n.) One or more distributed services that define the unique functionality provided by Java Enterprise System. System services normally require the support of a number of suppliers and/or a number of shared components.

system service component (n.) One of a number of kinds of system components included in Java Enterprise System. System services components provide the main Java Enterprise System infrastructure services: portal services, communication and collaboration services, identity and security services, web and application services, and availability services.

T

tag (n.) In XML documents, a piece of text that describes a unit of data or an element. The tag is distinguishable as markup, as opposed to data, because it is surrounded by angle brackets (< and >). To treat such markup syntax as data, you use an entity reference or a `CDATA` section.

takeover See failover.

target (1) (n.) In the context of access control, the target identifies the directory information to which a particular ACI applies.

(2) (n.) In the Application Server, a target is a server instance to which an application deployment or configuration change applies.

(3) (n.) In Apache Ant, a target is a set of tasks you want to be executed. See also `asant`, build file.

target entries (n.) The entries within the scope of a CoS.

task (n.) In Calendar Express on the client side, a component of a calendar that specifies something to be done. On the server side, a task is also called a todo.

taxonomy (n.) A system of categories for the resources in the Java Enterprise System Portal Server Search Engine.

telnet proxy (n.) An application that sits between the telnet client and telnet server and acts as an intelligent relay.

template (n.) A set of formatting instructions that apply to the nodes selected by an XPath expression.

template entry See cooperating server.

timeout (n.) A specified time after which the server should give up trying to finish a service routine that appears to be hung.

time zone (n.) A geographical region that uses the same time. There are 25 hourly time zones from -12 through +12 (GMT is 0). Each time zone is measured relative to GMT. Most time zones have localized designations in three-letter abbreviations. The Calendar Server also identifies time zones using a time zone ID (TZID) such as America/Los_Angeles or Asia/Calcutta.

TLS (Transport Layer Security) (n.) A protocol that provides encryption and certification at the transport layer so that data can flow through a secure channel without requiring significant changes to the client and server applications. The standard for SSL, a public key-based protocol.

todo (n.) On the server side, a component of a calendar that specifies something to be done. In Calendar Express on the client side, a todo is called a task.

tool provider (n.) An organization or software vendor that provides tools used for the development, packaging, and deployment of J2EE applications.

top (n.) (UNIX only) A program on some UNIX systems that shows the current state of system resource usage.

topic (n.) An object created by an administrator to implement the publish and subscribe delivery model. A topic can be viewed as a node in a content hierarchy that is responsible for gathering and distributing messages addressed to it. By using a topic as an intermediary, message publishers are kept separate from message subscribers.

top-level administrator (n.) A user who has administrative privileges to create, modify, and delete mail users, mail lists, family accounts, and domains in an entire Messaging Server namespace by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs. By default, this user can act as a message store administrator for all messaging servers in the topology.

top-level domain authority (n.) The highest category of host name classification, usually signifying either the type of organization the domain is (for example, `.com` is a company and `.edu` is an educational institution) or the country of its origin (for example, `.us` is the United States, `.jp` is Japan, `.au` is Australia, and `.fi` is Finland).

topology (1) (n.) The way a directory tree is divided among physical servers and how these servers link with one another.

(2) (n.) An arrangement of machines, Application Server instances, and HADB nodes, and the communication flow among them. See server instance, HADB node.

transaction (1) (n.) A set of database commands that succeed or fail as a group. All the commands involved must succeed for the entire transaction to succeed.

(2) (n.) An atomic unit of work that modifies data. A transaction encloses one or more program statements, all of which complete with either a commit or a rollback. Transactions enable multiple users to access the same data store concurrently.

transaction attribute (n.) A value specified in an enterprise bean's deployment descriptor that is used by the EJB container to control the transaction scope when the enterprise bean's methods are invoked. A transaction attribute can have the following values: `Required`, `RequiresNew`, `Supports`, `NotSupported`, `Mandatory`, or `Never`.

transaction context (n.) A transaction's scope, either local or global. See transaction context

transaction isolation level (n.) The degree to which the intermediate state of the data being modified by a transaction is visible to other concurrent transactions and data being modified by other transactions is visible to it.

transaction manager (n.) Provides the services and management functions required to support transaction demarcation, transactional resource management, synchronization, and transaction context propagation. Normally uses the XA protocol. See also global transaction.

transaction recovery (n.) Automatic or manual recovery of distributed transactions.

transience (n.) A protocol that releases a resource when it is not being used. Opposite of persistence.

transient failure (n.) An error condition that occurs during message handling. The remote MTA is unable to handle the message when the message is delivered but might be able to handle the message later. The local MTA returns the message to the queue and schedules the message for retransmission at a later time.

Transport Layer Security (TLS) (n.) The standardized form of SSL. See also secure socket layer.

transport protocols (n.) Protocols which provide the means to transfer messages between MTAs, for example SMTP and X.400.

trust database (n.) A security file that contains the public and private keys. Also referred to as the key-pair file.

trusted provider (n.) One of a group of service providers and identity providers in a circle of trust. Users can transact and communicate with trusted providers in a secure environment.

U

UAProf (n.) A specification defined by the Open Mobile Alliance that allows a mobile device to communicate its capabilities to a network server.

UBE See unsolicited bulk email.

UDDI (Universal Description, Discovery, and Integration) (n.) Provides worldwide registry of web services for discovery and integration. An industry initiative to create a platform-independent, open framework for describing services, discovering businesses, and integrating business services using the Internet, as well as a registry. It is being developed by a vendor consortium.

Unicode (n.) A 16-bit character set defined by ISO 10646 and the Unicode Consortium that maps digits to characters in languages around the world. Because 16 bits covers 32,768 codes, Unicode is large enough to include all the world's languages, with the exception of ideographic languages that have a different character for every concept, such as Chinese. All source code in the Java programming environment is written in Unicode. For more information, see `http://www.unicode.org/`.

unified messaging (n.) The concept of using a single message store for email, voicemail, fax, and other forms of communication. Java Enterprise System Messaging Server provides the basis for a complete unified messaging solution.

uniform resource indicator See URI.

uninstallation (n.) The process of removing a software component in its entirety.

universal principal name (n.) The value for a logged-in user that includes the login name combined with the domain to which the user belongs. For example, a user `bill` in domain `example.com` has the Universal Principal Name of `bill@example.com`. Also known as UPN.

Universal Standard Products and Services Classification (UNSPSC)

(n.) A schema that classifies and identifies commodities. It is used in sell-side and buy-side catalogs and as a standardized account code in analyzing expenditure.

unparsed entity

(n.) A general entity that contains something other than XML. By its nature, an unparsed entity contains binary data.

unsolicited bulk email

(n.) Unrequested and unwanted email sent from bulk distributors usually for commercial purposes. Also known as spam.

upper reference

(n.) Indicates the directory server that holds the naming context above your directory server's naming context in the DIT.

URI

(uniform resource identifier) (n.) A globally unique identifier for an abstract or physical resource. A URL is a kind of URI that specifies the retrieval protocol (`http` or `https` for Web applications) and physical location of a resource (host name and host-relative path).

URL database repair

(n.) A process that repairs and updates a URL database that has been damaged by a software failure, a system crash, a disk breakdown, or a full file system.

URL mapping

(n.) The process of mapping a document directory's physical path name to a user-defined alias so that files within the directory need only refer to the directory's alias instead of the file's full physical path name. Instead of identifying a file as `usr/JES/servers/docs/index.html`, you could identify the file as `/myDocs/index.html`. This mapping provides additional security for a server by eliminating the need for users to know the physical location of server files.

URL path

(n.) The part of a URL passed by an HTTP request to invoke a servlet. A URL path consists of the context path, servlet path, and path info, as follows:

- The context path is the path prefix associated with a servlet context of which the servlet is a part. If this context is the default context rooted at the base of the web server's URL namespace, the path prefix will be an empty string. Otherwise, the path prefix starts with a `/` character but does not end with a `/` character.
- The servlet path is the path section that directly corresponds to the mapping that activated this request. This path starts with a `/` character.
- The path info is the part of the request path that is not part of the context path or the servlet path.

URL pool

(n.) The list of URLs for the robot to process. When the robot starts, the URL pool consists of the starting points, but the pool is quickly augmented with any resources found during enumeration.

URN (uniform resource name) (n.) A unique identifier that identifies an entity but doesn't tell where it is located. A system can use a URN to look up an entity locally before trying to find it on the web. It also allows the web location to change, while still allowing the entity to be found.

use case (n.) A specific end-user task or set of tasks performed by a distributed enterprise application, and used as a basis for designing, testing, and measuring the performance of the application.

user (1) (n.) A person or service which uses an application. Programmatically, a user consists of a user name, password, and set of attributes that enables an application to recognize a user.

(2) (n.) An individual (or application program) identity that has been authenticated. A user can have a set of roles associated with that identity, which entitles the user to access all resources protected by those roles. See also principal, group, and role.

user account (n.) An account for accessing a server maintained as an entry on a directory server.

userAgent (n.) For Portal Server Mobile Access, a property that refers to the HTPP user-agent header. The user-agent header is often unique to a particular mobile device and can be used to detect and retrieve data for a client type.

user agent (n.) The client component, such as Netscape™ Communicator, that allows users to create, send, and receive mail messages. Also known as UA.

user data constraint (n.) Indicates how data between a client and a web container should be protected. The protection can be the prevention of tampering with the data or prevention of eavesdropping on the data.

user entry (n.) Fields that describe information about each user, required and optional. Examples are distinguished name, full name, title, telephone number, pager number, login name, password, home directory, and so on. Also known as user profile.

user folders (n.) A user's email mailboxes.

user group (n.) The group to which the user of a Message Queue client belongs for purposes of authorizing access to Message Queue message server resources, such as connections and destinations.

User/Groups Directory Server (n.) A Directory Server that maintains information about users and groups in an organization.

user quota (n.) The amount of space configured by the system administrator that is allocated to a user for email messages.

user provisioning (n.) The process by which services are made available to end users or by which end users are provided with access to services. Provisioning involves identity, policy, and user account

management activities, such as creating an account in a directory for each end user and populating the account with the user-specific information needed by various services.

user session (n.) A series of user application interactions that are tracked by the server. Sessions maintain user state, persistent objects, and identity authentication.

V

valid (adj.) A valid XML document, in addition to being well formed, conforms to all the constraints imposed by a DTD. It does not contain any tags that are not permitted by the DTD, and the order of the tags conforms to the DTD's specifications.

validating parser (n.) A parser that ensures that an XML document is valid in addition to being well formed.

value-binding expression (n.) A JavaServer Faces expression language expression that refers to a property of a backing bean. A component tag uses this expression to bind the associated component's value or the component instance to the bean property. If the component tag refers to the property via its value attribute, then the component's value is bound to the property. If the component tag refers to the property via its binding attribute then the component itself is bound to the property.

vanity domain (n.) A domain name associated with an individual user and not with a specific server or hosted domain. A vanity domain is specified by using the `MailAlternateAddress` attribute. The vanity domain does not have an LDAP entry for the domain name. Vanity domains are useful for individuals or small organizations that desire a customized domain name without the administration overhead of supporting their own hosted domain. Also called custom domain.

/var/mail (n.) A name often used to refer to Berkeley-style inboxes in which new mail messages are stored sequentially in a single, flat text file.

versioning See dynamic reloading.

virtual data view (n.) An LDAP representation of a JDBC data source, LDIF data source, or multiple aggregated data sources. A virtual data view is essentially a regular Directory Proxy Server data view on which certain transformation actions have been defined.

virtual domain (1) (n.) An ISP-hosted domain.

(2) (n.) A domain name added by the Messaging Multiplexor to a client's user ID for LDAP searching and for logging into a mailbox server. See also domain

virtual host (n.) Multiple hosts plus domain names mapped to a single IP address.

virtual list view index (n.) A filtering method which speeds up the display of entries in the Directory Server Console (or other graphical user interface) if the client with the user interface uses the virtual list view extension. Virtual list view indexes can be created on any branch in the directory tree to improve display performance for specific searches. Also known as the browsing index.

virtual private network (n.) A network with the appearance and functionality of a regular network but which is similar to a private network within a public one. The use of encryption in the lower protocol layers provides a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than true private networks using private lines. VPNs rely on having the same encryption system at both ends. The encryption might be performed by firewall software or possibly by routers.

virtual server (1) (n.) A virtual web server that serves content targeted for a specific URL. Multiple virtual servers can serve content using the same or different host names, port numbers, or IP addresses. The HTTP service can direct incoming web requests to different virtual servers based on the URL. Also known as a virtual host.

(2) (n.) Virtual servers are a way of setting up multiple domain names, IP addresses, and server monitoring capabilities with a single installed server.

virtual server class (n.) A collection of virtual servers that share the same basic configuration information in a `obj.conf` file.

virtual transformation (n.) A definition that determines how physical data is displayed in a Directory Proxy Server virtual data view. A virtual transformation is defined on a data view, in order to obtain a different view of the data.

voice Portal Desktop (n.) The audio presentation of a Portal Server site as presented by a telephone or similar device.

voiceXML (n.) A markup language for creating audio dialogues for interactive voice response applications.

VoIP (voice over IP) (n.) Technology that provides voice telephony over IP networks.

volume manager (n.) A software product that provides data reliability through disk striping, concatenation, mirroring, and dynamic growth of metadevices or volumes.

VPN See virtual private network.

VPN gateway (n.) The entry point to a VPN. Typically protected by a firewall.

VRFY (n.) An SMTP command for verifying a user name. Defined in RFC 821.

W

W3C (World Wide Web Consortium) (n.) The international body that governs Internet standards. Its Web site is `http://www.w3.org/`.

WAP (Wireless Application Protocol) (n.) An open standard that runs applications through wireless communications.

WAR file See web application archive.

warning (n.) A SAX parser warning is generated when the document's DTD contains duplicate definitions and in similar situations that are not necessarily an error but which the document author might like to know about, because they could be. See also fatal error.

WCAP (Web Calendar Access Protocol) (n.) A high-level, command-based protocol used by clients to communicate with the Calendar Server.

web application (n.) A collection of servlets, pages created with JSP technology, HTML documents, and other web resources, which might include image files, compressed archives, and other data. A web application can be packaged into a web archive (a WAR file) or exist in an open directory structure. Java Enterprise System Application Server also supports some non Java web application technologies, such as SHTML and CGI.

web application archive (n.) An archive file that contains a complete web application in compressed form. Java Enterprise System Web Server cannot access an application in a WAR file. You must decompress a web application (deploy it using the `wdeploy` utility) before Java Enterprise System Web Server can serve it.

web application, distributable (n.) A web application that uses J2EE technology written so that it can be deployed in a web container distributed across multiple Java virtual machines running on the same host or different hosts. The deployment descriptor for such an application uses the `distributable` element.

web cache (n.) A Java Enterprise System Application Server feature that enables a servlet or a page created with JSP technology to cache its results for a specific duration in order to improve performance. Subsequent calls to that servlet or JSP page within the duration are given the cached results so that the servlet or JSP page does not have to execute again.

web component (n.) A component that provides services in response to requests; either a servlet or a JSP page.

web connector plug-in (n.) An extension to a web server that enables the web server to communicate with the Java Enterprise System Application Server.

web container (n.) A container that implements the web component contract of the J2EE architecture. This contract specifies a runtime environment for web components that includes security, concurrency, life-cycle management, transaction, deployment, and other services. A web container provides the same services as a JSP container as well as a federated view of the J2EE platform APIs. A web container is provided by a web or J2EE server.

web container, distributed (n.) A web container that can run a web application that is tagged as `distributable` and that executes across multiple Java virtual machines running on the same host or on different hosts.

web container provider (n.) A vendor that supplies a web container.

webmail (n.) A generic term for browser-based email services. A browser-based client, known as a "thin" client because more processing is done on the server, accesses mail that is always stored on a server. See also Messenger Express.

web module (n.) A web application that is deployed individually, as opposed to within a J2EE application. See web application.

web resource (n.) A static or dynamic object contained in a web application that can be referenced by a URL.

web resource collection (n.) A list of URL patterns and HTTP methods that describe a set of Web resources to be protected.

Web Server (n.) A web server in Portal Server that is used as the web container for Portal Server and Portal Server pack web applications. Sun Java System Web Server is included with the Directory Server Access Management Edition product.

web server (n) A host that provides services to access the Internet, an intranet, or an extranet, and that stores and manages web applications, but not full J2EE applications. A web server hosts web sites, provides support for HTTP and other protocols, and executes server-side programs (such as CGI scripts or servlets) that perform certain functions. In the J2EE architecture, a web server provides services to a web container. For example, a web container typically relies on a web server to provide HTTP message handling. The J2EE architecture assumes that a web container

is hosted by a web server from the same vendor, so it does not specify the contract between these two entities. A web server can host one or more web containers.

web server plug-in (n.) An HTTP reverse proxy plug-in that allows you to instruct a Java Enterprise System Web Server or Java Enterprise System Application Server to forward certain HTTP requests to another server.

web server provider (n.) A vendor that supplies a web server.

web service (1) (n.) A service that conforms to standardized Internet protocols for accessibility, service encapsulation, and discovery. The standards include the SOAP (Simple Object Access Protocol) messaging protocol, the WSDL (Web Service definition Language) interface definition, and the UDDI (Universal Discovery, Description, and Integration) registry standard. A web service accepts a request, performs its function based on the request, and returns a response. The request and the response can be part of the same operation, or they can occur separately, in which case the consumer does not need to wait for a response. Both the request and the response usually take the form of XML, a portable data-interchange format, and are delivered over a wire protocol, such as HTTP.

(2) (n.) A service offered through the web. A self-contained, self-describing, modular application that can accept a request from a system across the Internet or an intranet, process it, and return a response.

web service consumer (n.) A web service consumer invokes the operations a Web service provides by making a request to a Web service provider.

web service provider (n.) A web service provider implements a Web service based on a request from a Web service consumer. It may run on the same Java™ virtual machine as the Web service consumer using it.

well-formed (adj.) An XML document that is syntactically correct. It does not have any angle brackets that are not part of tags, all tags have an ending tag or are themselves self-ending, and all tags are fully nested. Knowing that a document is well-formed makes it possible to process it. However, a well-formed document may not be valid. To determine validity, you need a validating parser and a DTD.

Windows CGI (n.) (Windows NT only) CGI programs written in a Windows-based programming language such as Visual Basic.

wireless desktop dispatcher (n.) A component that determines to which Portal Desktop, mobile Portal Desktop, or voice Portal Desktop user requests are routed.

withdrawn patch (n.) A patch which has been removed from distribution systems.

WML (wireless markup language) (n.) A markup language based on XML which is part of the WAP.

workgroup (n.) Local workgroup environment, where the server performs its own routing and delivery within a local office or workgroup. Interdepartmental mail is routed to a backbone server. See also backbone.

WS-BPEL (web services business process execution language) (n.) A variant of BPEL that uses constructs derived from the web services description language (WSDL). Using these constructs, WS-BPEL describes inbound and outbound process interfaces so that a process can easily be integrated into other processes or applications.

WSDL (web services description language) (n.) An XML-based language used to define web services in a standardized way. Describes three fundamental properties of a web service: definition of the web service, how to access that web service, and the location of that web service.

X through Z

X.400 (n.) A message handling system standard.

X.500 standard (n.) The set of ISO/ITU-T documents outlining the recommended information model, object classes, and attributes used by Directory Server implementation. LDAP is a lightweight version of the Directory Access Protocol (DAP) used by the X.500 standard.

Xalan (n.) An interpreting version of XSLT.

XA protocol (n.) A database industry standard protocol for distributed transactions.

XHTML (extensible hypertext markup language) (n.) A reformulation of HTML 4.0 which can be extended by adding new elements and attributes. An XML look-alike for HTML defined by one of several XHTML DTDs. To use XHTML for everything would of course defeat the purpose of XML, because the idea of XML is to identify information content, and not just to tell how to display it. You can reference it in a DTD, which allows you to say, for example, that the text in an element can contain `<em>` and `<b>` tags rather than being limited to plain text.

XLink (n.) The part of the XLL specification that is concerned with specifying links between documents.

XLL (n.) The XML Link Language specification, consisting of XLink and XPointer.

XML (extensible markup language) (n.) A flexible programming language developed by the World Wide Web Consortium (W3C) to create common information formats and to share both the format and the data on the web, intranets, and elsewhere. This markup language allows you to define the tags (markup) needed to identify the content, data, and text in XML documents. It differs from HTML, the markup language most often used to present information on the Internet. HTML has fixed tags that deal mainly with style or presentation. An XML document must undergo a transformation into a language with style tags under the control of a style sheet before it can be presented by a browser or other presentation mechanism. Two types of style sheets used with XML are CSS and XSL. Typically, XML is transformed into HTML for

presentation. Although tags can be defined as needed in the generation of an XML document, a document type definition (DTD) can be used to define the elements allowed in a particular type of document. A document can be compared by using the rules in the DTD to determine its validity and to locate particular elements in the document. A Web services application's J2EE deployment descriptors are expressed in XML with schemas defining allowed elements. Programs for processing XML documents use SAX or DOM APIs. The Calendar Server uses XML and XSL to generate the Calendar Express user interface.

XML namespace (n.) A standard that allows you to specify a unique label to the set of element names defined by a DTD (document type definition). A document using that DTD can be included in any other document without having a conflict between element names. The elements defined in the DTD are then uniquely identified so that, for example, the parser can determine when an element should be interpreted according to your DTD and not according to that of another document type definition.

XML registry See registry.

XML schema (n.) The W3C specification for defining the structure, content, and semantics of XML documents.

XPath (n.) An addressing mechanism for identifying the parts of an XML document.

XPointer (n.) The part of the XLL specification that is concerned with identifying sections of documents so that they can be referenced in links or included in other documents.

XSL (extensible style language) (n.) A language used to create style sheets for XML, similar to cascading style sheets (CSS) that are used for HTML. In XML, content and presentation are separate. XML tags do not indicate how they should be displayed. An XML document has to be formatted before it can be read. The XSL standard lets you do the following:

- Specify an addressing mechanism, so that you can identify the parts of an XML document that a transformation applies to (XPath).
- Specify tag conversions, so that you can convert XML data into different formats (XSLT).
- Specify display characteristics, such page sizes, margins, and font heights and widths, as well as the flow objects on each page. Information fills in one area of a page and then automatically flows to the next object when that area fills up. That allows you to wrap text around pictures, for example, or to continue a newsletter article on a different page (XSL-FO).

XSL-FO (n.) A subcomponent of XSL used for describing font sizes, page layouts, and how information flows from one page to another.

XSLT (extensible style language transformation) (n.) The language used by XML style sheets to transfer one form of an XML document to another XML form. This transition is extremely

useful in e-commerce and e-business, as the transition serves as a common denominator across many different platforms and varying XML document coding. The target document often has presentation-related tags dictating how it will be rendered by a browser or other presentation mechanism. XSLT was formerly a part of XSL, which also included a tag language of style flow objects.

XSLTC (n.) A compiling version of XSLT.

Zulu time (n.) A military designation for GMT and UTC (coordinated universal time).